B.30

NOT MEASUREMENT SENSITIVE

MIL-STD-882C
19 January 1993
SUPERSEDING
MIL-STD-882B
30 March 1984
w\ NOTICE 1
1 July 1987
MIL-STD-1574A
15 August 1979

MILITARY STANDARD

SYSTEM SAFETY PROGRAM REQUIREMENTS

AMSC Number F6861

FSC SAFT

1. This military standard is approved for use by all Departments and Agencies of the Department of Defense.

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: HQ Air Force Materiel Command (SES), 4170 Hebble Creek Rd. Suite 1, Wright-Patterson AFB, OH 45433-5644, by using the self-addressed Standardization Document Improvement Proposal (DD Farm 1426) appearing at the end of this document or by letter.

3. The principle objective of a system safety program within the Department of Defense (DOD) is to make sure safety, consistent with mission requirement, is included in technology development and designed into systems, subsystems, equipment, facilities, and their interfaces and operation.

4. DOD has approved this military standard for all DOD departments to use in developing system safety programs in accordance with DOD Instructions. Selective application and the tailoring of this military standard must be accomplished, as indicated herein to specify the extent of contractual and DOD inhouse compliance.

5. The degree of safety achieved in a system depends directly on management emphasis. Government agencies and contractors will apply management emphasis to safety during the system acquisition process and throughout the life cycle of each system, making sure mishap risk is understood and risk reduction is always considered in the management review process.

6. A formal safety program that stresses early hazard identification and elimination or reduction of associated risk to a level acceptable to the managing activity is the principal contribution of effective system safety. The success of the system safety effort depends on definitive statements of safety objectives and requirements.

TABLE PAGE

FIGURE PAGE

APPENDICES

A. GUIDANCE FOR IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

PARAGRAPH PAGE

SYSTEM SAFETY PROGRAM REQUIREMENTS

1. SCOPE

1.1 Scope. This standard applies to all DOD systems and facilities. It applies to every activity of the system life cycle; e.g., research, technology development, design, test and evaluation, production, construction, checkout/calibration, operation, maintenance and support, modification and disposal The requirements will also he applied to DOD in-house programs.

1.2 Purpose. This standard provides uniform requirements for developing and implementing a system safety program of sufficient comprehensiveness to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps. The system safety program addresses hazards from many sources to include system design, hazardous materials, advancing technologies, and new techniques. The aim is to eliminate hazards or reduce the associated risk to a level acceptable to the managing activity (MA). The term "managing activity" usually refers to the Government procuring activity, but may include prime or associate contractors or subcontractors who impose system safety tasks on their suppliers

1.3 Application.

1.3.1 Applying the standard. The sections and tasks shall he selectively tailored and applied as described below. In the event that a contractual document only specifies compliance with "MIL-STD-882C" and does not stipulate specific sections or tasks, the tailoring specified in paragraph 5.3 shall apply. The term "section" herein means the top paragraph and all its subparagraphs/tasks.

1.3.2 Applying tasks Tasks described in this standard shall he selectively applied in DOD contract-definitixed procurements, requests for proposal (RFP), statements of work (SOW), and Government in-house developments requiring system safety programs for the development, test, production, and deployment of systems, facilities, and equipment. The word "contractor" herein also includes Government activities developing military systems, equipment, and facilities.

1.3.2.1 Application guidance. Application guidance and rationale for selecting tasks to fit the needs of a particular system safety program are included in the appendices. These appendices are generally not contractually binding; however, the MA may choose to impose portions of Appendix B or C as part of Task 101.

1.3.2.2 Method of referencing the tasks of this standard as contractual requirements, both this standard and each specific task number are to he cited. Applicable "Details To Be Specified" will be included in the SOW.

2. APPLICABLE DOCUMENTS.

This standard contains no reference documents. Applicable documents required to supplement this military standard must be specified in system specifications and other contractual documents.

3. ACRONYMS AND DEFINITIONS.

3.1 Acronyms used in this standard. The acronyms used in this standard are defined as follows:

a. AE - Architect and Engineering Firm

b. CDRL - Contract Data Requirements List

c. CFR - Code of Federal Regulations

d. CSP - Certified Safety Professional

e. DEHCP - DOD Explosive Hazard Classification Procedures

f. DID - Data Item Description

g. DLA - Defense Logistic8 Agency

h. DOD - Department of Defense

i. DoDI - DOD Instruction

j. DOT - Department of Transportation

k. ECP - Engineering Change Proposal

l. ECPSSR - Engineering Change Proposal System Safety Report

m. EOD - Explosive Ordnance Disposal

n. EPA - Environmental Protection Agency

o. ESMCR - Eastern Space and Missile Center Regulation

p. GFE - Government-Furnished Equipment

q. GFP - Government-Furnished Property

r. GIDEP - Government-Industry Data Exchange Program

s. HHA - Health Hazard Assessment

t. HHAR - Health Hazard Assessment Report

u. HRI - Hazard Risk Index

v. IRS - Interface Requirements Specifications

w. ISSPP - Integrated System Safety Program Plan

x. MA - Managing Activity

y. MIL-STD - Military Standard

z. MRAR - Mishap Risk Assessment Report

aa. MSGSAP- Missile System Ground Safety Approval Package

ab. MSPRP - Missile System Prelaunch safety Package

ac. NDI - Nondevelopmental Item

ad. O&SHA - Operating & Support Hazard Analysis

ae. OPR - Office of Primary Responsibility

af. OSHA - Occupational Safety and Health Administration

ag. PE - Professional Engineer

ah. PI-IA - Preliminary Hazard Analysis

ai. PHL - Preliminary Hazard List

aj. PM - Program Manager

ak. P/N - Part Number

al. RFP - Request for Proposal

am. SAR - Safety Assessment Report

an. SCCSC - Safety Critical Computer Software Components

ao. SCN - Specification Change Notice

ap. SCG - Storage Compatibility Group

aq. SDR - System Design Review

ar. SHA - system Hazard Analysis

as. SHRI - Software Hazard Risk index

at. SOW - Statement of Work

au. SPR - Software Problem Report

av. SRCA - Safety Requirements/Criteria Analysis

aw. SRR - System Requirements Review

ax. SRS - Software Requirements Specifications

ay. SSG - System Safety Group

az. SSHA - Subsystem Hazard Analysis

ba. SSPP - System Safety Program Plan

bb. SSPPR - System Safety Program Progress Report

bc. SSR - Software Specification Review

bd. SSS - System/Segment Specification

be. SSWG - System Safety Working Group

bf. TBD - To Be Determined

bg. TLV - Threshold Limit Value

bh. WDSSR - Waiver or Deviation System Safety Report

bi. WSMCR - Western Space and Missile Center Regulation

3.2 Definitions. The following definitions apply:

3.2.1 Condition. An existing or potential state such as exposure to harm, toxicity, energy source, activity, etc.

3.22 Contractor. A private sector enterprise or the organizational element of DOD or any other Government agency engaged to provide services or products within agreed limits specified by the MA.

3.2.3 Fail safe. A design feature that ensures that the system remains safe or in the event of a failure will cause the system to revert to a state which will not cause a mishap.

3.2.4 Hazard. A condition that is prerequisite to a mishap.

3.2.5 Hazard probability. The aggregate probability of occurrence of the individual events that create a specific hazard.

3.2.6 Hazard severity. An assessment of the consequences of the worst credible mishap that could be caused by a specific hazard.

3.2.7 Hazardous Material. Anything that due to its chemical, physical, or biological nature causes safety, public health, or environmental concerns that result in an elevated level of effort to manage.

3.2.8 Managing activity. The organizational element of DOD assigned acquisition management responsibility for the system, or prime or associate contractors or subcontractors who impose system safety tasks on their suppliers.

3.2.9 Mishap. An unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment Accident

3.2.10 Nondevelopmental item.

a. Any item of supply that is available in the commercial marketplace;

b. Any previously developed item of supply that is in use by a department or agency of the United States, a State or local government, or a foreign government with which the United States has a mutual defense cooperation agreement;

c. Any item of supply described in definition a. or b. , above, that requires only minor modification in order to meet the requirements of the procuring agency; or

d. Any item of supply that is currently being produced that does not meet the requirements of definition a, b., or c., above, solely because of the item is not yet in use or is not yet available in the commercial marketplace.

33.11 Risk. An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability.

3.2.12 Risk assessment. A comprehensive evaluation of the risk and its associated impact.

3.2.13 Safety. Freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.

3.2.14 Safety critical. A term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe *system* operation or use; e.g., safety critical function, safety critical path, safety critical component.

32.15 Safety critical computer software components. Those computer software components and units whose errors can result in a potential hazard, or loss of predictability or control of a system.

3.2.16 Subsystem. An element of a system that, in itself may constitute a system.

32.17 System. A composite, at any level of complexity, of personnel, procedures, materials, tools, equipment, facilities, and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement.

3.2.18 System safety. The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

3.2.19 System safety engineer. An engineer who is qualified by training and/or experience to perform system safety engineering tasks.

3.2.20 System safety engineering. An engineering discipline requiring specialized professional knowledge and skills in applying scientific and engineering principles, criteria, and techniques to identify and eliminate hazards, in order to reduce the associated risk.

32.21 System safety group/working group. A formally chartered group of persons, representing organizations initiated during the system acquisition program, organized to assist the MA system program manager in achieving the system safety objectives. Regulations of the military components define requirements, responsibilities, and memberships.

32.22 System safety management. A management discipline that defines system safety program requirements and ensures the planning, implementation and accomplishment of system safety tasks and activities consistent with the overall program requirements.

3223 System safety manager. A person responsible to program management for setting up and managing the system safety program.

3.2.24 System safety program. The combined tasks and activities of system safety management and system safety engineering implemented by acquisition project managers.

3.226 System safety program plan. A description of the planned tasks and activities to be used by the contractor to implement the required system safety program. This description includes organizational responsibilities, resources, methods of accomplishment, milestones, depth of effort, and integration with other program engineering and management activities and related systems.

4. GENERAL REQUIREMENTS.

4.1 System safety program. The contractor shall establish and maintain a system safety program to support efficient and effective achievement of overall system safety objectives.

4.1.1 Management system. The contractor shall establish a safety management system to implement provisions of this standard commensurate with the program contractual requirements. The contractor program *manager shall be* responsible for the establishment, control, incorporation, direction and implementation of the system safety program policies and shall assure that mishap risk is identified and eliminated or controlled within established program risk acceptability parameters. The contractor shall establish internal reporting systems and procedures for investigation and disposition of system related mishaps and safety incidents, including potentially hazardous conditions not yet involved in a mishap/incident. Report such matters to the MA as required by the contract

4.1.2 Key system safety personnel. The contractor shall establish and maintain a key system safety position for each program. The individual in this position shall be directly responsible to the contractor program manager for safety matters and shall meet the minimum qualifications specified by the MA

4.1.3 Compliance. Compliance with all contractually imposed requirements of this standard is mandatory. When a requested system safety program plan is approved by the MA, it provides a basis of understanding between the contractor and tbe MA as to how the system safety program will be accomplished. Any deviation must be requested by the contractor and approved by the MA.

4.1.4 Conflicting requirements. When conflicting requirements or deficiencies are identified within system safety program requirements or with other program requirements, the contractor shall submit notification, with proposed solutions or alternatives and supporting rationale, to the MA for resolution.

4.2 System safety program objectives. The *system safety program shall* define a systematic approach to make sure that:

a. Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.

b. Hazards associated with each system are identified, tracked, evaluated, and eliminated, or the associated risk reduced to a level acceptable to the MA throughout the entire life cycle of a system. Risk shall be described in risk assessment terms (see paragraph 4.5 below).

c. Historical safety data, including lessons learned from other systems, are considered and used.

d. Minimum risk is sought in accepting and using new technology, materials or designs; and new production, test and operational techniques.

e. Actions taken to eliminate hazards or reduce risk to a level acceptable to the MA are documented.

f. Retrofit actions required to improve safety are minimized through the timely

inclusion of safety features during research, technology development for and acquisition of a system.

g. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to the MA

h. Consideration is given early in the life cycle to safety and ease of disposal (including explosive ordnance disposal), and demilitarization of any hazardous materials associated with the system. Actions should be taken to minimize the use ofhaxardous materials and, therefore, minimize the risks and life cycle costs associated with their use.

i. Significant safety data are documented as "lessons learned" aud are submitted to data banks or as proposed changes to applicable design handbooks and specifications.

4.3 System safety design requirements. System safety design requirements will be specified after review of pertinent standards, specifications, regulations, design handbooks, safety design checklists, and other sources of design guidance for applicahihty to the design of the system. The contractor shall establish safety design criteria derived from all applicable data including the preliminary hazard analyses if available. This criteria shall be the basis for developing system specification safety requirements. The contractor shall continue to expand the criteria aud requirements for inclusion in development specification during the subsequent program phases. Some general system safety design requirements are:

a Eliminate identified hazards or reduce associated risk through design, including material selection or substitution. When potentially hazardous materials must be used, select those with least risk throughout the life cycle of the system.

b. Isolate hazardous substances, components, and operations from other activities, areas, personnel, and incompatible materials.

c. Locate equipment so that access during operations, servicing, maintenance, repair, or adjustment minimizes personnel exposure to hazards (e.g., hazardous chemicals, high voltage, electromagnetic radiation, cutting edges, or sharp points).

d. Minimize risk resulting from excessive environmental conditions (e.g., temperature, pressure, noise, toxicity, acceleration and vibration).

e. Design to minimize risk created by human error in the operation and support of the system.

f. Consider alternate approaches to minimize risk from hazards that cannot he eliminated. Such approaches include interlocks, redundancy, fail safe design, system protection, fire suppression, and protective clothing, equipment, devices, and procedures_

g. Protect the power sources, controls and critical components of redundant subsystems by physical separation or shielding.

h. When alternate design approaches cannot eliminate the hazard, provide safety and warning devices and warning and caution notes in assembly, operations, maintenance, and repair instructions, and distinctive markings on hazardous components and materials, equipment, and facilities to ensure personnel and equipment protection. These shall be standardized in accordance with commonly accepted industry or military practice or with MA requirements for conditions in which prior standards do not exist.

The MA shall be provided copies of all warnings, cautions and distinctive markings proposed for review and comment.

i. Minimize the severity of personnel injury or damage to equipment in the event of a mishap.

j. Design software controlled or monitored functions to minimize initiation of hazardous events or mishaps.

k. Review design criteria far inadequate or overly restrictive requirements regarding safety. Recommend new design criteria supported by study, analyses, or test data.

4.4 System safety precedence. The order of precedence for satisfying system safety requirements and resolving identified hazards shall he as follows:

4.4.1 Design for [redacted] From the first, design to eliminate hazards. If an identified hazard cannot be eliminated, reduce the associated risk to an acceptable level, as defined by the MA, through design selection.

4.4.2 Incorporate safety devices. If identified hazards cannot he eliminated or their associated risk adequately reduced through design selection, that risk shall be reduced to a level acceptable to the MA through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks of safety devices when applicable.

4.4.3 Provide warning devices. *When* neither design nor safety devices can effectively eliminate identified hazards or adequately reduce associated risk, devices shall be used to detect the condition and to produce an adequate warning signal to alert personnel of the hazard. Warning signals and their application shall be designed to minimize the probability of incorrect personnel reaction to the signals and shall he standardized within like types of systems.

4.44 Develop procedures and training. Where it is impractical to eliminate hazards through design selection or adequately reduce the associated risk with safety and warning devices, procedures and training shall be used. However, without a specific waiver from the MA, no warning, u&ion, or other form of written advisory shall be used as the only risk reduction method for Category I or II hazards (as defined in paragraph 4.5.1 below). Procedures may include the use of personal protective equipment. Precautionary notations shall be standardized as specified by the MA. Tasks and activities judged to be safety critical by the MA may require certification of personnel proficiency.

4.5 Ri[redacted]t. Decisions regarding resolution of identified hazards *shall be* based on assessment of the risk involved To aid the achievement of the objectives of system safety, hazards shall be characterized as to hazard severity categories and hazard probability levels, when possible. Since the priority for system safety is eliminating hazards by design, a risk assessment procedure considering only hazard severity will generally suffice during the early design phase to minimize risk. When hazards are not eliminated during the early design phase, a risk assessment procedure based upon the hazard probability, hazard severity, as well as risk impact, shall be used to establish priorities for corrective action and resolution of identified hazards.

4.5.1 **Hazard severity.** Hazard severity categories are defined to provide a qualitative measure of the worst credible mishap resulting from personnel error; environmental conditions; design inadequacies; procedural deficiencies; or system, subsystem or component failure or malfunction as shown at Table 4.1.

TABLE 1. HAZARD SEVERITY CATEGORIES

Description	Category	Definition
CATASTROPHIC	I	Death, system loss, or severe environmental damage.
CRITICAL	II	Severe injury, sever8 occupational illness, major system or environmental damage.
MARGINAL	III	Minor injury, minor occupational illness, or minor system or environmental damage.
NEGLIGIBLE	IV	Less than minor injury, occupational illness, or less than minor system or environmental damage.

NOTE: These hazard severity categories provide guidance to a wide variety of programs. However, adaptation to a particular program is generally required to provide a mutual understanding between the MA and the contractors as to the meaning of the terms used in the category definitions. The adaptation must define what constitutes system loss, major or minor system or environmental damage, and severe and minor injury and occupational illness. Other risk assessment techniques may be used provided they are approved by the MA

4.62 **Hazard probability.** The probability that a hazard will be created during the planned life expectancy of the system can be described in potential occurrences per unit of time, events, population, items, or activity. Assigning a quantitative hazard probability to a potential design or procedural hazard is generally not possible early in the design process. A qualitative hazard probability may be derived from research, analysis, and evaluation of historical safety data from similar systems. Supporting rationale for assigning a hazard probability shall be documented in hazard analysis reports. An example of a qualitative hazard probability ranking is shown at Table 4.2.

TABLE 2. HAZARD PROBABILITY LEVELS

Description*	Level	Specific Individual Item	Fleet or Inventory**
FREQUENT	A	Likely to occur frequently	Continuously experienced
PROBABLE	B	Will occur several times in the life of an item.	Will occur frequently
OCCASIONAL	C	Likely to occur some time in the life of an item	Will occur several times
REMOTE	D	Unlikely but possible to occur in the life of an item	Unlikely but can reasonably be expected to occur
IMPROBABLE	E	So unlikely, it can be assumed occurrence may not be experienced	Unlikely to occur, but possible

*Definitions of descriptive words may have to be modified based on quantity involved.
**The size of the fleet or inventory should be defined.

4.5.3 Risk impact. The risk impact shall be assessed, as necessary, to discriminate between hazards having the same hazard risk index. This impact consists of the effect and cost of an identified risk in terms of mission capabilities, and social, economic and political factors. (Example- Release of small amount ofradioactive material may not cause direct physical damage or equipment damage, but can cause extreme damage socially and politically to a program.)

4.6 Action on identified hazards. Action shall be taken to eliminate identified hazards or reduce the associated risk to a level defined by or acceptable to the MA. Catastrophic, critical and other hazards specified by the MA shall not rely solely on warnings, cautions or procedures/training for control of risk. If this is impossible or impractical, alternatives shall be recommended to the MA.

4.6.1 Residual risk. The risk associated with significant hazards for which there are no known control measures, no plans to control or incomplete control measures will be considered residual risk. The contractor will document each residual risk along with the reason(s) for incomplete resolution and notify the MA

5. DETAILED REQUIREMENTS.

5.1 General. The detailed requirements are presented as tasks. The tasks are located in four task sections: Section 100, Program Management and Control, Section 200, Design and Integration; Section 300, Design Evaluation; and Section 400, Compliance and Verification. The groupings and order are intended to assist in application of the various tasks, but it is not intended that the tasks or subtasks be accomplished in the sequence presented. The sequence of task and subtask accomplishment should be tailored to the individual program to which they are being applied.

5.2 Task Structure. Each individual task is divided into three parts: purpose, task description, and details to be specified.

a The purpose provides a brief reason for performing the task.

b. Tbe task description provides the actual subtasks that comprise the task a contractor shall perform if specified by the MA. Task descriptions shall be tailored by the MA as required by governing regulations and as appropriate to particular systems or equipment, program type, magnitude, and funding. In tailoring the tasks, the detail and depth of the effort is defined by the MA and incorporated in the appropriate contractual documents. When preparing proposals, the contractor may include additional tasks or task modifications with supporting rationale for each addition or modification.

c. Tbe "Details to be Specified" paragraph under each task description lists specific details, additions, modifications, deletions, or options to the requirements of the task that should be considered by the MA when tailoring the task description to fit program needs. This information is then included in the document in which the task is invoked. The list provided with each task is not necessarily complete and may be supplemented by the MA "Details to be Specified" annotated by an "(R)" are required and must be provided to the contractor by the MA for proper implementation of the task, if the task is to be contractually implemented.

5 . 3 Tailoring for paragraph 1.3.1 provision. When this paragraph is invoked, the following tasks in this standard are required to be performed and are tailored as follows:

a. Task 101. Comply with all of Section 4. Figure 1, Appendix A, shall be used to prioritize hazards and determine the acceptable level of risk.

b. Task 102. The SSPP shall be contractually binding when approved by the MA

c. Task 103. The MA shall be integrator if integration among contractors is necessary.

d. Task 105. The contractor shall be a technical advisor to the SSG. The contract shall support one SSG, a test review meeting and two other safety meetings per contract year. This support shall include briefing assigned topics at these meetings and answering questions related to the system safety effort

e. Task 106. The contractor shall maintain a hazard log of all hazards initially ranked as a Category I, II or III (Catastrophic, Critical or Marginal) severity.

f. Task 107. The contractor shall prepare quarterly progress reports.

g. Task 202. The PHA shall be used to identify potential hazards associated with the system.

h. Task 301. The SAR shall be used to manage safety in test planning and conduct.

i Task 302. The contractor shall comply with all local range safety requirements. The contractor shall complete requirements of this task 120 days prior to planned test start.

j. Task 303. The contractor shall notify the MA safety representative by phone within one working day of identifying a change in the hazard severity or probability by one level.

k. Task 401. Safety critical items shall include command and control elements of a system, subsystem or component; fuzes, firing circuits, and safe and arm devices for ordnance; and any hardware, software or procedures that controls risk for Category I or II (Catastrophic or Critical) severity hazards.

6.0 NOTES.

(This section contains information of a general or explanatory nature which may be helpful, but is not mandatory.)

6.1 Intended use. This standard is a source of requirements for establishing a system safety program.

6.2 Data requirements. See Appendix D.

6.3 Tailoring guidance for contractual application. See Appendix A.

6.4 Identification of changes. Margin notations are not used in this revision to identify changes with respect to the previous issue due to the extensiveness of the changes.

CONCLUDING MATERIAL

Custodians:
Army - AV
Navy - AS
Air Force - 10

Reviewing Activities:
Army - AT, SC, AR, MI, SG
Navy - OS, SH, YD, SA, EC
Air Force - 11, 13, 19, 26

Preparing Activity
Air Force - 10

Project SAFT-0026)

TASK SECTION 100

PROGRAM MANAGEMENT AND CONTROL

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 101

SYSTEM SAFETY PROGRAM

101.1 **PURPOSE**. The purpose of Task 101 is to establish the foundation for a system safety program. The total system safety program consists of this task plus any other tasks from Sections 100, ZOO, 300,400 or other source designated by the MA

101.2 **TASK DESCRIPTION**.

101.2.1 Establish and execute a system safety program which meets the tailored requirements of Section 4, GENERAL REQUIREMENTS, and all other tasks/requirements designated by the MA.

101.22 Develop a planned approach for safety task accomplishment, provide qualified people to accomplish the tasks, establish the authority for implementing the safety tasks through all levels of management, and allocate appropriate resources, both manning and funding, to assure the safety tasks are completed.

101.2.3 Establish a system safety organization or function and lines of communication within the program organization and with associated organizations (government and contracted). Establish interfaces between system safety and other functional elements of the program, as well as between other safety disciplines such as nuclear, range, **explosive, chemical, biological, etc. Designate the organizational unit responsible for executing each safety task. Establish the** authority for resolution of identified hazards.

101.2.4 Define system safety program milestones and relate these to major program milestones, program element responsibility, and required inputs and outputs.

101.2.5 Establish an incident alerting/notification, investigation and reporting process, to include notification of the MA

101.3 **DETAILS TO BE SPECIFIED**.

101.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Task 101.

(R) b. Tailoring of Section 4 to meet specific program requirements.

(R) c. Acceptable level of risk with reporting thresholds.

(R) d. Minimum hazard probability and severity reporting thresholds.

e. MA requirements for incident processing.

f. Requirement for and methodology of reporting to the MA the following:

(1) Residual hazards/risks.

(2) Safety critical characteristics and features.

(3) Operating, maintenance and overhaul safety requirements.

(4) Measures used to abate hazards.

(5) Acquisition management of hazardous materials.

g. Qualifications for key system safety personnel.

h. Other specific system safety program requirements.

SYSTEM SAFETY PROGRAM PLAN

102.1 PURPOSE. The purpose of Task 102 is to develop a System Safety Program Plan (SSPP). It shall describe in detail tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate/control hazards, or reduce the associated risk to a level acceptable to the MA throughout the system life cycle. The approved plan provides a formal basis of understanding between the contractor and MA on how the system safety program will be executed to meet contractual requirements, including general and specific provisions.

102.2 TASK DESCRIPTION. The contractor shall develop a SSPP to provide a basis of understanding between the contractor and the MA as to how the system safety program will be accomplished to meet contractual safety requirements included in the general and special provisions of the contract. The approved plan shall, on an item-by-item basis, account for all contractually required tasks and responsibilities, including those in the Statement of Work (SOW). The SSPP shall include the following:

102.2.1 Program scope and objectives. Each SSPP shall describe, as a minimum, the four elements of an effective system safety program: a planned approach for task accomplishment, qualified people to accomplish tasks, authority to implement tasks through all levels of management, and appropriate commitment of resources (both manning and funding) to assure tasks are completed The SSPP shall define a program to satisfy the system safety requirements imposed by the contract. This se&ion shall:

a. Describe the scope of the overall program and the related system safety program.

b. List the tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety identify where they are specified or described.

c. Account for all contractually required safety tasks and responsibilities. A matrix shall be provided to correlate the requirements of the contract to the location in the SSPP where the requirement is addressed.

1022.2 System safety organization. The SSPP shall describe:

a. The system safety organization or function within the organization of the total program using charts to show the organizational and functional relationships, and lines of communication. The organizational relationship between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization shall be shown. Review and approval authority of applicable tasks by system safety shall be described.

b. The responsibility and authority of system safety personnel, other contractor organizational elements involved in the system safety effort, subcontractors, and system safety groups. Describe the methods by which safety personnel may raise issues of concern directly to the program manager or the program manager's supervisor within the corporation. Identify the organizational unit responsible for

executing each task. Identify the authority in regard to resolution of all identified hazards.

c. The staffing of the system safety organization for the duration of the contract to include manpower loading, control of resources and a summary of the qualifications of key system safety personnel assigned to the effort, including those who possess coordination/approval authority for contractor prepared documentation.

d. The procedures by which the contractor will integrate and coordinate the system safety efforts including assignment of the system safety requirements to action organizations and subcontractors, coordination of subcontractor system safety programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.

e. The process through which contractor management decisions will be made including timely notification ofunacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, program deviations, etc.

f. Details of how resolution and action relative to system safety will be effected at the program management level possessing resolution authority.

102.2.3 System safety program milestones. The SSPP shall:

a. Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.

b. Provide a program schedule of safety tasks including start and completion dates, reports, and reviews.

c. Identify subsystem, component, software safety activities as well as integrated system level activities (i.e., design analyses, tests, and demonstrations) applicable to the system safety program but specified in other engineering studies and development efforts to preclude duplication.

d. Provide the estimated manpower loading required to complete each task.

102.2.4 General system safety requirements and criteria. The SSPP shall:

a. Describe general engineering requirements and design criteria for safety. Describe safety requirements for support equipment and operational safety requirements for all appropriate phases of the life cycle up to, and including, disposal. List the safety standards and system specifications containing safety requirements that shall be complied with by the contractor. Include titles, dates, and where applicable, paragraph numbers.

b. Describe the risk assessment procedures. The hazard severity categories, hazard probability levels, and the system safety precedence that shall be followed to satisfy the safety requirements of the program. State any qualitative or quantitative measures of safety to be used for risk assessment including a description of the

acceptable/unacceptable risk levels. Include system safety definitions which modify, deviate from or are in addition to those in this standard.

c. Describe closed-loop procedures for taking action to resolve identified unacceptable risk including those involving nondevelopmental items.

102.2.5 Hazard analysis. The SSPP shall describe:

a. The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met.

b. The depth within the system to which each technique is used including hazard identification associated with the system, subsystem., components, software, hazardous materials, personnel, ground support equipment, nondevelopmental items, facilities, and their interrelationship in the logistic support, training, maintenance, operational and disposal (including render safe and emergency disposal) environments.

c. The integration of subcontractor hazard analyses with overall system hazard analyses.

d. Efforts to identify and control hazards associated with materials used during the system's life cycle.

102.2.6 System safety data. Tbe SSPP shall:

a Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned, data

b. Identify deliverable data by title and number, and means of delivery (e.g. hard copy, electronically, etc.).

c. Identify non-deliverable system safety data and describe the procedures for accessibility by the MA and retention of data of historical value.

102.2.7 Safety verification. The SSPP shall describe:

a. The verification (test, analysis, inspection, etc.1 requirements for making sure that safety is adequately demonstrated. Identify any certification requirements for software, safety devices or other special safety features (e.g., render safe and emergency disposal procedures).

b. Procedures for making sure safety-related verification information is transmitted to the MA for review and analysis.

c. Procedure for ensuring the safe conduct of all tests.

102.2.8 Audit program. The SSPP shall describe the techniques and procedures to be employed by the contractor to make sure the objectives and requirements of the system safety program are being accomplished.

102.2.9 **Training.** The SSPP shall describe the safety training for engineering, technician, operating and maintenance personnel.

102.2.10 Incident reporting. The contractor shall describe in the SSPP the mishap/incident alerting/notification, investigation and reporting process including notification of the MA

102.2.11 System safety interfaces. The SSPP shall identify, in detail:

a. The interface between system safety and all other applicable safety disciplines such as: nuclear safety, range safety, explosive and ordnance safety, chemical and biological safety, laser safety and any others.

b. The interface between system safety, systems engineering, and all other support disciplines such as: maintainability, quality control, reliability, software development, human factors engineering, medical support (health hazard assessments), and any others.

c. The interface between system safety and all system integration and test disciplines.

102.3 **DETAILS TO BE SPECIFIED.**

102.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a Imposition of Tasks 101 and 102.

(R) b. Identification of contractual status of the SSPP; i.e., if the MA wants the SSPP to be contractually binding, a statement to that effect must be placed in the statement of work.

c. Identification of additional information to be provided.

TASK 103

INTEGRATIONMANAGEMENT OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS, AND ARCHITECT AND ENGINEERING FIRMS

103.1 PURPOSE. The purpose of Task 103 is to provide the system integrating contractor and MA with appropriate management surveillance of other contractors' system safety programs, and the capability to establish and maintain uniform integrated system safety program requirements. This task will also describe requirements for associate contractors, subcontractors, and architect and engineering firms' (AE) system safety programs. This task can also be used to require the flow down of system safety requirements to subcontractors, suppliers, and vendors.

103.2 TASK DESCRIPTION.

103.2.1 Integrating contractor. The contractor designated as integrator for the safety functions of all associate contractors shall:

a. Prepare an integrated system safety program plan (ISSPP) as the SSPP required by Task 102 defining the role of the integrator and the effort required from each associate contractor to help integrate system safety requirements for the total system. In addition to the other contractually imposed requirements, the plan shall address and identify:

(1) Definition of where the control, authority and responsibility transitions from Integrating Contractor to associates and subcontractors,

(2) Analyses, risk assessment, and verification data to be developed by each associate contractor with format and method to be utilized.

(3) Data each associate contractor is required to submit to the integrator and its scheduled delivery keyed to program milestones.

(4) Schedule and other information considered pertinent by the integrator.

(5) The method of development of system level (including software) requirements to be allocated to each of the associate contractors as a part of the system specification, end-item specifications, and other interface requirement documentation.

(6) Safety-related data pertaining to nondevelopmental items (NDI).

(7) Integrated safety analyses to be conducted and support required from associate and subcontractors.

(8) Integrating contractors' roles in test range, nuclear safety, explosive, or other certification processes.

b. Initiate action through the MA to make sure each associate contractor is required to be responsive to the ISSPP. Recommend contractual modification where the need

exists.

c. When conducting risk assessments, analyze the integrated system design, operations, and specifically the interfaces between the products of each associate contractor or subcontractor and the end item, Data or analyses provided by associate contractors and subcontractors shall be used in the conduct of this effort.

d. When performing a safety assessment, summarize the mishap risk presented by the operation of the integrated system. Data or analyses provided by associate contractors or subcontractors shall be used in the conduct of this effort.

e. Provide assistance and guidance to associate contractors regarding safety matters.

f. Resolve differences between associate contractors in areas related to safety, especially during development of safety inputs to system and item specifications. Where problems cannot be resolved by the integrator, notify the MA for resolution and action.

g. Initiate action through the MA to make sure information required by an associate contractor (from the integrating contractor or other associate contractors) to accomplish safety tasks, is provided in an agreed-to format.

h. Develop a method of exchanging safety information between contractors. If necessary, schedule and conduct technical meetings between all associate contractors to discuss, review, and integrate the safety effort Use of the SSG/SSWG meetings should be included as required.

i. Implement an audit program to make sure the objectives and requirements of the system safety program are being accomplished. Whenever the integrating contractor believes an associate contractor has failed to meet contract requirements, the integrating contractor will notify the MA in writing. The integrator for the safety effort will send a copy of the notification to the associate contractor.

103.2.2 Associate contractor. Associate contractors shall provide safety data and support (including participation in SSGs/SSWGs) needed by other associate contractors and the integrator to the extent specified in the contract

103.2.3 Subcontractors. Applicable provisions of this standard shall be included in all contracts with major subcontractors. The "chain of responsibility" for formally flowing down the system safety contractual requirements from the prime contractor to different levels of subcontractors, suppliers, and vendors (who provide different applicable subsystems, equipment and/or parts) shall be identified.

a. All subcontractors shall be required to maintain suitable documentation of safety analyses they have performed in formats which will permit incorporation of their data into the overall analysis program,

b. Major subcontractors shall be required to develop system safety program plans to be included as annexes to the prime contractor's SSPP.

c. Lesser subcontractors and vendors shall be required to provide information on software, component and subassembly characteristics, including failure modes, failure rates, and possible hazards, which will permit prime contractor personnel to evaluate the items for their impact on safety of the system.

d. All subcontractors shall participate in the SSG aud SSWGs, when required

103.2.4 Architect and engineering firms. The AE shall be responsible for conducting facility hazard analyses and other facility SSPP functions as specified in the SOW. The AE shall be responsible for securing the expertise necessary to perform the required work and will have the same responsibilities as a prime contractor in hazard identification, tracking, and resolution. The AE shall assure that design subcontractors or consultants maintain and provide suitable documentation of any safety analyses performed.

103.3 DETAILS TO BE SPECIFIED.

103.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101, 102 and 103 as tailored.

(R) b. Designation of the system safety integrating contractor.

c. Designation of status of the other contractors.

d. Requirements for any special integrated safety analyses.

e. Requirements to support test range, nuclear safety, explosive, environmental or other certification processes.

f. Description of specific integration roles.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 104

SYSTEM SAFETY PROGRAM REVIEWS/AUDITS

104.1 **PURPOSE.** The purpose of Task **104** is to establish a requirement for the contractor to perform and document system safety program **reviews/audits or** support of reviews/audits performed by the **MA.** This **task is also** used to acquire support for special requirements such as **certifications** and **test/flight** readiness reviews.

104.2 **TASK DESCRIPTION.**

104.2.1 The contractor shall perform and document system safety program reviews/audits as specified by the **MA.** These reviews/audits shall be performed on:

a. The contractor's system safety program.

b. The associate contractors' system safety program(s).

c. The support contractors' system safety program(s).

d. The subcontractors' system safety program(s).

104.2.2 The contractor shall support system safety **reviews/audits** performed by representatives of the MA to the extent specified in the SOW.

104.2.3 To the extent specified by the MA in the SOW, the contractor **shall** support presentations **to** Government **certifying** activities such as phase safety reviews, munitions safety boards, nuclear safety hoards, or flight safety review boards. These may also include special reviews such as flight/article readiness reviews or preconstruction briefings.

104.3 **DETAILS TO BE SPECIFIED.**

104.3.1 Details **to** be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 104.

(R) b. Identification of reviews/audits, their content, and probable location(s).

c. Method of documenting the results of system safety reviews/audits.

d. Frequency of system safety reviews/audits.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 105

SYSTEM SAFETY GROUP/SYSTEM SAFETY WORKING GROUP SUPPORT

105.1 **PURPOSE.** The purpose of **Task** 105 is to *require* contractors to support System safety Groups **(SSGs)** and System Safety Working Groups **(SSWGs)** which are established in accordance with service regulations or as otherwise defined by the **MA.**

1052 **TASK DESCRIPTION.** The contractor shall participate as an active member of MA **SSG/SSWGs.** Such participation shall include activities specified by the MA such as:

a. Presenting the contractor safety program status, including results of design or operations risk assessments.

b. Summarizing hazard analyses including identification of problems, status of resolution, and residual risk.

c. Presenting incident assessments (especially mishaps and malfunctions of the system being acquired) results including recommendations and action taken to prevent recurrences.

d. Responding to action items assigned by the chairman of the **SSG/SSWG.**

e. Developing and validating system safety requirements and criteria applicable to the program.

f. Identifying safety deficiencies of the program and providing recommendations for corrective actions or preventions of reoccurrence.

g. Planning and coordinating support for a required certification process.

h. Documenting and distributing of meeting agendas and minutes.

105.2.1 Subcontractors. The contractor shall require that all major subcontractors participate in the SSWSSWGs.

105.2.2 **Associate Contractor.** The integrating contractor shall require that all associate contractors participate in the SSWSSWGs.

105.3 **DETAILS TO BE SPECIFIED.**

105.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 105.

(R) b. Contractor membership requirements and role assignments, e.g., recorder, member, alternate, or technical advisor.

(R) c. Frequency or total number of **SSG/SSWG** meetings and probable locations.

d. Specific **SSG/SSWG** or other presentation support tasks.

THIS PAGE INTENTIONALLY LEFTBLANK

TASK 106

HAZARD TRACKING AND RISK RESOLUTION

106.1 **PURPOSE.** The purpose of Task 106 is to establish a single closed-loop hazard tracking system.

106.2 **TASK DESCRIPTION.** The contractor shall develop *a* method *or* procedure to document and track hazards and their controls thus providing an audit trail of hazard resolutions. A centralized file, computer data base or document called a "Hazard Log" shall be maintained. The "Hazard Log" shall contain as a minimum:

a Description of each hazard to include associated hazard risk index.

b. Status of each hazard and control.

c. Traceability of resolution on each Hazard Log item from the time the hazard was identified to the time the risk associated with the hazard was reduced to a level acceptable to the MA.

d. Identification of residual risk.

e. Action person(s) and organizational element.

f. The recommended controls to reduce the hazard to a level of risk acceptable to the MA.

g. The signature of the MA accepting the risk and thus effecting closure of the Hazard Log item.

106.3 DETAILS TO BE SPECIFIED.

106.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 106.

(R) b. Procedure by, and detail to, which hazards are entered into the log..

(R) c. Procedure by which the contractor shall obtain close-out or risk acceptance by the MA of each hazard.

d. Complete set of data required on the hazard log, including format.

e. Identification of any special requirements involving a computerized log.

THIS PAGE **INTENTIONALLY LEFT BLANK**

TASK 107

SYSTEM SAFETY PROGRESS SUMMARY

107.1 **PURPOSE.** The purpose of Task 107 is to prepare a periodic progress report summarizing the pertinent system safety management and engineering activity that occurred during the **reporting** period.

107.2 **TASK DESCRIPTION.** The contractor shall prepare a periodic system safety progress report summarizing general progress made relative to the **system** safety program during the specified reporting period, and projected work for the next **reporting** period. The report shall contain the following information:

a. A brief summary of activities, progress, and status of the safety effort in relation to the scheduled program milestones. It shall highlight significant achievements and problems. It shall include progress toward completion of safety data prepared or in work.

b. Newly recognized significant **hazards** and significant changes in the degree of control of the risk of known hazards.

c. Individual hazard resolution status and status of all recommended corrective actions that have not been implemented.

d. Significant cost and schedule changes that impact the safety program.

e. Discussion of contractor documentation reviewed by the system safety **function** during the reporting period. Indicate whether the documents were acceptable for content and whether or not inputs to improve the safety posture were made.

f. Proposed agenda items for the next system safety group/working group meeting, if such groups are formed.

107.3 **DETAILS TO BE SPECIFIED.**

107.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 107.

(R) b. Specification of progress reporting period.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK SECTION 200

DESIGN AND INTEGRATION

THIS PAGE INTENTIONALLY LEFT BLANK

PRELIMINARY HAZARD LIST

201.1 **PURPOSE.** The purpose of Task 201 is to compile a preliminary hazard list (PHL) very early (or to update the PHL later) in the system acquisition life cycle to identify potentially hazardous areas on which to put management emphasis.

2012 **TASK DESCRIPTION.** The contractor shall:

201.2.1 Examine the system shortly after the concept definition effort begins and compile a PHL identifying possible **hazards** that may be inherent in the concept and their associated mishap potential, or hazards specified by the MA

201.2.2 Review safety experience on similar systems, including mishap/incident hazard tracking logs (if accessible), safety lessons learned, etc., to identify possible hazards and their mishap risks. The sources of a hazards found in this review shall be referenced in the PHL.

201.2.3 Further investigate selected hazards or hazardous characteristics **identified** in the **PHL** as directed by the MA to determine their significance.

201.3 **DETAILS TO BE SPECIFIED.**

201.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 201.

b. Identification of special concerns, hazards, or undesired events the MA wants listed or investigated.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 202

PRELIMINARY HAZARD ANALYSIS

202.1 **PURPOSE.** The purpose of Task 202 is to perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions.

202.2 **TASK DESCRIPTION.** The contractor shall perform and document a preliminary hazard analysis to obtain an initial risk assessment of a concept or system. Based on the best available data, including mishap data (if assessable) from similar systems and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to the MA shall be included. The PHA shall consider the following for identification and evaluation of hazards as a minimum:

a Hazardous components (e.g., fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources).

b. Safety related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This shall include consideration of the potential contribution by software (including software developed by other contractors/sources) to subsystem/system mishaps. Safety design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or MA-designated undesired events) shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.

c. Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation).

d. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage). Those test unique hazards which will be a direct result of the test and evaluation of the article or vehicle.

e. Facilities, real property installed equipment, support equipment (e.g., provisions for storage, assembly, checkout, prooftesting of hazardous systems/assemblies which may involve toxic, flammable, explosive, corrosive or cryogenic materials/wastes; radiation or noise emitters; electrical power sources) and training (e.g. training and certification pertaining to safety operations and maintenance).

f. Safety related equipment, safeguards, and possible alternate approaches (e.g.,

interlocks; system **redundancy;** fail safe design considerations using hardware or **software** controls; subsystem protection; fire **detection** and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning, and noise or radiation barriers).

g. Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of **hazard** determined, and appropriate specification and/or design **changes** developed.

202.3 DETAILS TO BE SPECIFIED.

202.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition **of** Tasks 101 and 202.

(R) b. Minimum hazard probability and severity reporting thresholds.

c. Any selected hazards, hazardous areas, or other specific items to be examined or excluded.

TASK 203

SAFETYREQ - CRITERIA ANALYSIS

203.1 PURPOSE. The purpose of Task 203 is to perform and document the safety design requirements/design criteria for a facility or system under development/design.

203.2 TASK DESCRIPTION. The Safety Requirements/Criteria Analysis (SRCA) relates the hazards identified to the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level. The SRCA uses the Preliminary Hazard List (Task 201) or the Preliminary Hazard Analysis (Task 202) as a basis, if available. The SRCA is also used to incorporate design requirements that are safety related but not tied to a specific hazard. The analysis includes the following efforts:

203.2.1 The contractor shall determine applicable generic system safety design requirements and guidelines for facilities; hardware and software from federal, military, national and industry regulations, codes, standards, specifications; and other documents for the system under development. The contractor shall incorporate these requirements and guidelines into the high level system specifications and design documents as appropriate.

203.2.2 The contractor shall analyze the System Design Requirements, System/Segment Specifications (SSS), Preliminary Hardware Configuration Item Development Specification, Software Requirements Specifications (SRS), and the Interface Requirements Specifications (IRS), or equivalent documents as appropriate, to include the following sub-tasks:

a The contractor shall ensure that the system safety design requirements and guidelines are developed; refined; correctly and completely specified; properly translated into system hardware and software requirements and guidelines where appropriate; and implemented in the design and development of the system hardware and associated software.

b. The contractor shall identify hazards and relate them to the specifications or documents listed above and develop design requirements to reduce the risk of those hazards.

c. The contractor shall identify safety critical computer software components (SCCSCs) and ensure they are placed under configuration control.

d. The contractor shall analyze the preliminary system design to identify potential hardware/ software interfaces at a gross level that may cause or contribute to potential hazards. Interfaces identified shall include control functions, monitoring functions, safety systems and functions that may have indirect impact on safety. These interfaces and the associated software shall be designated as safety critical.

e. The contractor shall perform a preliminary hazard risk assessment on the identified safety critical software functional requirements using the hazard risk matrix or software hazard criticality matrix of Appendix A or another process as mutually agreed to by the contractor and the MA

f. The contractor shall ensure that System Safety design requirements are properly incorporated into the operator, user, and diagnostic manuals.

203.2.3 The contractor shall develop safety related design change recommendations and testing requirements and shall incorporate them into Preliminary Design Documents and the hardware, software and system test plans. The following sub-tasks shall be accomplished:

a The contractor shall develop safety-related change recommendations to the design and specification documents listed above and shall include a means of verification for each design requirement.

b. The contractor shall develop safety related test requirements for incorporation into the test documents. Tests shall be developed for hardware, software and system integration testing.

203.2.4 The contractor shall support the System Requirements Review (SRR), System Design Review (SDR) and Software Specification Review (SSR) from a system safety viewpoint. The contractor shall address the system safety program, analyses performed and to be performed, significant hazards identified, hazard resolutions or proposed resolutions, and means of verification.

203.3 DETAILS TO BE SPECIFIED.

203.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 203 tailored to the developmental program.

(R) b. Definition of acceptable level of risk within the context of the system, subsystem, or component under analysis.

(R) c. Level of contractor support required for design reviews.

d. Specification of the type(s) of risk assessment process.

TASK 204

SUBSYSTEM HAZARD ANALYSIS

204.1 **PURPOSE.** The purpose of Task 204 is to perform and document a Subsystem Hazard Analysis (SSHA) to: verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents; identify previously unidentified hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem; recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels.

204.2 **TASK DESCRIPTION.** The contractor shall perform and document a subsystem hazard analysis to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements.. This will include government furnished equipment, nondevelopmental items, and software. Areas to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. The human shall be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct of this analysis.

204.2.1 The analysis shall include a determination:

a Of the modes of failure including reasonable human errors as well as single point and common mode failures, and the effects on safety when failures occur in subsystem components.

b. Of potential contribution of hardware and software (including that which is developed by other contractors/sources) events, faults, and occurrences (such as improper timing) on the safety of the subsystem.

c. That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied.

d. That the method of implementation of hardware, software, and facilities design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has it introduced any new hazards or risks.

e. Of the implementation of safety design requirements from top level specifications to detailed design specifications for the subsystem. The implementation of safety design requirements developed as part of the PHA and SRCA shall be analyzed to ensure that it satisfies the intent of the requirements.

f. Of test plan and procedure recommendations to integrated safety testing into the hardware and software test programs.

g. That system level hazards attributed to the subsystem are analyzed and that adequate control of the potential hazard is implemented in the design.

204.2.2 If no specific analysis techniques are directed or if contractor recommends that a different technique than specified by the MA should be used, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis.

204.2.3 When software to be used in conjunction with the subsystem is being developed under DOD-STD-2167 and DOD-SIB2168; or MIL-STD-1679 or other development documents; the contra&or performing the SSHA shall monitor, obtain and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA. Problems identified which require the reaction of the software developer shall be reported to the MA in time to support the ongoing phase of the software development process.

204.2.4 The contra&r shall update the SSHA as a result of any system design changes, including software design changes, which affect system safety.

2 0 4 3 3

204.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a Imposition of Tasks 101 and 204.

(R) b. Minimum hazard severity and probability reporting thresholds.

c. The specific subsystems to be analyzed.

d. Any selected hazard, hazardous areas, or other specific items to be examined or excluded.

e. Specification of desired analysis technique(s) and/or format.

f. The MA shall provide the technical data on GFE to enable the contractor to accomplish the defined tasks.

TASK 205

SYSTEM HAZARD ANALYSIS

205.1 **PURPOSE.** The purpose of Task 205 is to perform and document a System Hazard Analysis (SHA) to: verify system compliance with safety requirements contained in system specifications and other applicable documents; identify previously unidentified hazards associated with the subsystem interfaces and system functional faults; assess the risk associated with the total system design, including software, and specifically of the subsystem interfaces; and recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

205.2 **TASK DESCRIPTION.** The contractor shall perform and document a system hazard analysis to identify hazards and assess the risk of the total system design, including software, and specifically of the subsystem interfaces.

205.2.1 This analysis shall include a review of subsystems interrelationships for:

a. Compliance with specified safety design criteria

b. Possible independent, dependent, and simultaneous hazardous events including system failures; failures of safety devices; common cause failures and events; and system interactions that could create a hazard or result in an increase in mishap risk..

c. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.

d. Design changes that affect subsystems.

e. Effects of reasonable human errors.

f. Determination:

(1) Of potential contribution of hardware and software(including that which is developed by other contractors/sources, or Commercial Off-The-Shelf hardware or software) events, faults and occurrences (such as improper timing) on safety of the system.

(2) That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied.

(3) That the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or degraded the safety of tbe system nor has introduced any new hazards.

205.2.2 If no specific analysis techniques are directed or if the contractor recommends that a different technique than specified by the MA should be used, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis. The SHA may be combined with and/or performed using similar techniques to those used for the SSHA.

205.2.3 When software to be used in conjunction with the system is being developed under

DOD-STD-2167 and DOD-STD-2168; or MIL-STD-1679 or other software development requirement documents, the contractor performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA. Problems identified which require the reaction of the software developer shall be report4 to the MA in time to support the ongoing phase of the software development process.

205.2.4 The contractor shall update the SHA as a result of any system design changes, including software design changes which affect system safety.

205.3 DETAILS TO BE SPECIFIED.

205.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a Imposition of Tasks 101 and 205.

(R) b. Minimum hazard severity and probability reporting thresholds.

c. Any selected hazards, hazardous areas, or other specific items to be examined or excluded.

d. Specification of desired analysis technique(s) and/or format.

TASK 206

OPERATING AND SUPPORT HAZARD ANALYSIS

206.1 **PURPOSE.** The purpose of Task 206 is to perform and document an Operating and Support Hazard Analysis (O&SHA), to evaluate activities for hazards or risks introduced into the system by operational and support procedures and to evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks.

206.2 **TASK DESCRIPTION.** The contractor shall perform and document an O&SHA to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering: the planned system configuration/state at each phase of activity; the facility interfaces; the planned environments (or ranges thereof); the supporting tools or other equipment, including software controlled automatic test equipment, specified for use; operational/task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements; and the potential for unplanned events including hazards introduced by human errors. The human shall be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis. The O&SHA must identify the safety requirements (or alternatives) needed to eliminate or control identified hazards, or to reduce the associated risk to a level which is acceptable under either regulatory or contractually specified criteria

206.2.1 The analysis shall identify:

a Activities which occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods.

b. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks.

c. Requirements for safety devices and equipment, including personnel safety and life support equipment

d. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape, render safe, explosive ordnance disposal, back-out, etc.), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication.

e. Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials.

f. Requirements for safety training and personnel certification.

g. Effects of nondevelopmental hardware and software across the interface with other system components or subsystems.

h. Potentially hazardous system states under operator control.

206.2.2 The O&SHA shall document system safety assessment of procedures involved in:

system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, demilitarization, and disposal.

206.2.3 If no specific analysis techniques are directed or if the contractor recommends that a different technique than specified by the MA should be used, the contractor shall obtain MA approval of technique(s) to be used prior to performing the analysis.

206.2.4 The contractor shall update the O&SHA as a result of any system design or operational changes.

266.3 DETAILS TO BE SPECIFIED.

206.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 266.

(R) b. Minimum hazard probability and severity reporting thresholds.

c. Specification of desired analysis technique(s) and/or format

d. The specific procedures to be evaluated (Reference 206.2.2).

HEALTH HAZARD ASSESSMENT

207.1 **PURPOSE**. The purpose of Task 207 is to perform and **document a Health** Hazard **Assessment (HHA) to identify health hazards, evaluate proposed hazardous materials, and propose** protective measures to reduce the associated risk **to** a level acceptable to the MA

207.2 **TASK DESCRIPTION**. A HHA **shall be** performed **and** documented to **identify health hazards and to recommend engineering controls, equipment, and/or protective procedures, to reduce the associated risk to a level acceptable to the MA An HHA shall also evaluate the hazards and costs due to system components materials, evaluate alternative materials for those** components, **and** recommend materials that reduce the associated risk. Materials will be evaluated if (because of **their physical, chemical, or biological characteristics; quantity; or** concentrations) they cause or contribute to adverse **effects** in organisms or off-spring, pose a substantial present or future danger **to** the environment, or result in damage to or loss of equipment or property during the systems life cycle. Assessments shall include consideration of the generation of hazardous wastes.

207.21 **Specific** health hazards and impacts **that shall** be considered include:

a Chemical hazards (e.g., hazardous materials that are flammable; **corrosive;** toxic; carcinogens or **suspected** carcinogens; **systemic** poisons; asphyxiants, **including** oxygen deficiencies; respiratory irritants; etc.).

b. Physical hazards **(e.g.,** acoustical energy, heat or cold stress, **ionizing** and **non-**ionizing radiation).

c. Biological hazards **(e.g.,** bacteria, fungi, etc.)

d. Ergonomic hazards (e.g., **lifting** requirements, task saturation, etc.)

e. **Other** hazardous, or potentially hazardous, materials that may be formed by the introduction of the system. or by the manufacture, test, maintenance or operation of the system.

207.2.2 The assessment shall address:

a. System, facility and personnel protective equipment design requirements (e.g., ventilation, noise attenuation, radiation barriers, etc.) to allow safe operation and maintenance. When feasible engineering designs are not available to reduce hazards to acceptable levels, alternative protective measures must be specified (e.g., protective clothing, specific operation or maintenance practices to reduce risk to an acceptable level).

b. Potential non or less hazardous material substitutions and projected handling and **disposal** issues. The **HHA** will discuss the rationale for using a **hazardous** materiel and long term effects **(such as potential** for personnel and environmental exposure, handling and disposal issued requirements, protection/ control measures, and life cycle costs) over a non or less hazardous material. The *effects* and costs should be considered over **the life of the systems, including the cost of handling and disposal.**

Identify potential non or leas hazardous alternatives if they exist and provide a justification why an alternative cannot be used

c. Hazardous material data The HHA shall describe the means for identifying and tracking information for each hazardous material.

2072.3 The HHA hazardous material evaluation shall:

a. Identify the hazardous materials by name(s) and stock numbers; the affected system components and processes; the quantity, characteristics, and concentrations of the materials in the system; and source documents relating to the materials.

b. Determine under which conditions the hazardous materials can release or emit materials in a form that may be inhaled, ingested, absorbed by living organisms, or leached into the environment and if the materials pose a health threat.

c. Characterize material hazards and determine reference quantities and hazard ratings. Acute health, chronic health, carcinogenic, contact, flammability, reactivity, and environmental hazards will be examined.

d. Estimate the expected usage rate of each hazardous material for each process or component for the subsystem, total system, and program-wide impact.

e. Recommend the disposition of each hazardous material identified. If for any scale of operation the reference quantity is exceeded by the estimated usage rate, material substitution or altered processes shall be considered to reduce risks associated with the material hazards while evaluating the impact on program costs.

207.3 DETAILS TO BE SPECIFIED.

207.3.1 Details to be specified in the SOW shall include the following as applicable:

(R) a. Imposition of Tasks 101 and 207.

(R) b. Minimum hazard severity and probability reporting thresholds.

c. Any selected hazards, hazardous areas, hazardous materials, or other specific items to be examined or excluded.

d. Specification of desired analysis techniques and/or report formats.

TASK SECTION 300

DESIGN EVALUATION

THIS PAGE INTENTIONALLY **LEFT BLANK**

TASK 301

SAFETY ASSESSMENT

301.1 **PURPOSE.** The purpose of Task 301 is to perform and document a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system prior to the next contract phase or at contract completion.

301.2 TASK DESCRIPTION. The contractor shall perform and document a safety assessment to identify all safety features of the hardware, software, and system design and to identify procedural, hardware and software related hazards that may be present in the system being acquired including specific procedural controls and precautions that should be followed. The safety assessment shall summarize:

a The safety criteria and methodology used to classify and rank hazards, plus any assumptions on which the criteria or methodologies were based or derived including the definition of acceptable risk as specified by the MA

b. The results of analyses and tests performed to identify hazards inherent in the system, including:

(1) Those hazards that still have a residual risk, and the actions that have been taken to reduce the associated risk to a level contractually specified as acceptable.

(2) Results of tests conducted to validate safety criteria, requirements and analyses.

c. The results of the safety program efforts. Include a list of all significant hazards along with specific safety recommendations or precautions required to ensure safety of personnel, property, or the environment. Categorize the list of hazards as to whether or not they may be expected under normal or abnormal operating conditions.

d. Any hazardous materials generated by or used in the system, including:

(1) Identification of material type, quantity, and potential hazards.

(2) Safety precautions and procedures necessary during use, packaging, handling, storage, transportation, and disposal (e.g., explosive ordnance disposal). Include all explosives hazard classifications.

(3) After launch safety-related activity of expendable launch vehicles and their payloads including deployment, operation, reentry, and recovery **(if required) of launch vehicles/payloads which do not attain orbit (either planned or unplanned).**

(4) Orbital safety hazard awareness associated with space systems such as explosions, electromagnetic interference, radioactive sources, ionizing radiation, chemicals, space debris, safe separation distances between space vehicles, and natural phenomena.

(5) A copy of the Material safety Date Sheet (OSHA Form 174, or equivalent manufacturer6 format).

e. Conclude with a signed statement that all identified hazards have been eliminated or their associated risks controlled to levels contractually specified as acceptable, and that the system is ready to test or operate or proceed to the next acquisition phase. In addition, the contractor shall make recommendations applicable to hazards at the interface of his system with the other system(s) as contractually required.

301.3. DETAILS TO BE SPECIFIED.

301.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a Imposition of Tasks 101 and 301.

b. Define the specific purpose of the requested assessment.

c. Identify at what level (system safety manager, program manager, etc.) the statement (paragraph 301.2e) must be signed.

TASK 302

TEST AND EVALUATION SAFETY

302.1 **PURPOSE.** The purpose of Task 302 is to make sure safety is considered (and safety responsibility assigned) in test and evaluation, to provide existing analysis reports and other safety data, and to respond to all safety requirements necessary for testing in-house, at other contractor facilities, and at Government ranges, centers, or laboratories.

302.2 **TASK DESCRIPTION.** The contractor shall make sure the contractor test and evaluation safety activities recommend actions, and assess actions taken, to reduce, correct or control CATASTROPHIC- and CRITICAL-level hazards in the test and evaluation environment. MARGINAL or NEGLIGIBLE-level hazards shall also be addressed as required by the MA Specific test and evaluation safety activity tasks shall include the following

302.2.1 Test and evaluation planning. Planning for test and evaluation safety from the beginning of, and throughout, the contract period shall incorporate the following:

a Test program milestones requiring completion of hazard analyses, risk assessments, or other safety studies.

b. Schedule for analysis, evaluation, and approval of test plans, procedures, and other documents to make sure safety is covered during all testing.

c. Preparation of or input to safety, operating and test procedures.

d. Coverage of test equipment, installation of test equipment, end instrumentation in hazard analyses prior to test start.

e. Meeting specialized requirements designated by the MA and informing the MA of any identified hazards that are unique to the test environment.

f. Coordination and status reviews with the cognizant test site safety representatives to ensure test safety requirements are identified, monitored and completed as scheduled.

302.2.2 Safety reviews. Providing assistance to the safety review teams to the extent necessary to support a system safety certification process and validate, from a safety perspective, that the system is ready to test.

302.2.3 Follow-up actions.

a. Analyzing and documenting safety related test results.

b. Initiating follow-up action to insure completion of the corrective efforts taken to reduce, correct, or control test and evaluation hazards.

302.2.4 Reports. Maintaining a repository of test and evaluation hazard/action status reports.

302.3 **DETAILS TO BE SPECIFIED.**

302.3.1 Details to be specified in the SOW **shall include** the following, as applicable:

(R) a. Imposition of Tasks 101 and 302.

(R) b. Designation of applicable specialized system safety requirements for testing or use of range facilities.

(R) c. Schedule for meeting requirements designated in 302.2 above.

d. Identifkation of hazard categories for which activities will take action,

TASK 303

SAFETY REVIEW OF ENGINEERING CHANGE PROPOSALS, SPECIFICATION CHANGE NOTICES, SOFTWARE PROBLEM REPORTS, AND REQUESTS FOR DEVIATION/WAIVER

303.1 PURPOSE. The purpose of Task 303 is to perform and document analyses of Engineering Change Proposals (ECPs), Specification Change Notices (SCNs), Software Problem Reports (SPRs), program or software trouble reports (PTRs, STRs), and requests for deviation or waiver to determine the safety impact on the system.

303.2 **TASK DESCRIPTION.**

303.2.1 Engineering change proposals. The contractor shall analyze each ECP (as specified by the MA) to determine the hazards associated with it, assess the associated risk, and predict the safety impact of the ECP on the existing system. The contractor shall notify the MA when an ECP will decrease the level of safety of the existing system.

303.2.2 Specification change notices. The contractor shall analyze each SCN to determine the potential effect on safety critical component8 or subsystems. The contractor shall notify the MA if the level of safety of the system will be reduced.

303.2.3 S o f t w a r e . The contractor shall review each SPR to determine the potential safety implicationa If safety impact8 are identified, the contractor shall notify the MA of a decrease in the level of safety of the system.

303.2.4 **Requests for deviation/waiver.** The contractor shall analyze each request for deviation/waiver to determine the hazards and asses8 the risk of the proposed deviation from or waiver of a requirement, or a specified method or process. The change in the risk involved in accepting the deviation or waiver shall be identified. When the level of safety of the system will be reduced by deviation from, or waiver of the requirement, method, or process, the MA must be so notified.

303.3 **DETAILS TO BE SPECIFIED.**

303.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 303.

b. Specify amount of change in the level of safety requiring MA notification and the method and timing of such notification.

c. Identify class of ECP or type of deviation/waiver to which this task applies.

d. Identify who shall execute review and sign-off authority for each class of ECP or type of deviation/waiver.

THIS PAGE INTENTIONALLY LEFT BLANK

TASK SECTION 400

COMPLIANCE AND VERIFICATION

THIS PAGE INTENTIONALLY LEFT BLANK

TASK 401

SAFETY VERIFICATION

401.1 **PURPOSE.** The purpose of Task 401 is to **define** and perform tests and demonstrations or use other verification methods on safety critical hardware, software, and procedures to verify compliance with safety requirements.

401.2 **TASK DESCRIPTION.** The contractor shall define and perform tests, demonstrations, develop models, and otherwise verify the compliance of the system with safety requirements on safety critical hardware, software, and procedures (e.g., EOD and emergency procedures). Induced or simulated failures shall **be** considered **to** demonstrate the acceptable safety performance of the equipment and **software.** Where hazards are identified during the development **efforts** and analysis or inspection cannot determine the adequacy of actions **taken** to reduce the risk, safety tests shall be specified and conducted to evaluate the overall effectiveness of the actions taken. **SSPPs** and test plan and procedure documents shall be revised to include these tests. Where costs for safety testing would be prohibitive, safety characteristics or procedures may be verified by engineering analyses, analogy, laboratory test, functional mockups, or models and simulations, when approved by the **MA.** Specific safety tests shall be integrated into appropriate system test and demonstration plans, including verification and validation plans, to the maximum extent possible. Test plans, test procedures, and the results of all tests including design verification, technical operational evaluation, technical data and requirements validation and verification, production acceptance, and shelf-life validation shall be reviewed to make sure:

a Safety of the design (including operating and maintenance procedures) is adequately demonstrated, including verification of safety devices, warning devices, etc. for all CATASTROPHIC hazards not **eliminated** by design. CRITICAL, MARGINAL **and** NEGLIGIBLE hazards shall also be addressed as required by the **MA.**

b. Results of safety evaluations of the system are included in the test and evaluation reports on hardware or software.

401.3 **DETAILS TO BE SPECIFIED.**

401.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 401.

(R) b. Identification of safety critical equipment and procedures.

(R) c. Identification of hazard categories for which verification will be accomplished if paragraph **401.2a** is specified

d. Additional development of or inputs to test plans, procedures and reports **to** verify safety requirements.

THIS PAGE INTENTIONALLY LEFTBLANK

TASK 402

SAFETY COMPLIANCE ASSESSMENT

402.1 **PURPOSE.** The purpose of Task 402 is to perform and document an assessment to identify and verify compliance with military, federal, national, international, and industry codes to ensure safe design of a system, and to comprehensively evaluate the safety risk being assumed prior to test or operation of a system or at contract completion.

402.2 **TASK DESCRIPTION.** The contractor shall perform and document a safety compliance assessment to identity and document compliance with appropriate design and operational safety requirements. The assessment identifies the contractually imposed standards, specifications, and codes appropriate to the safety of the system and documents compliance with these requirements. The assessment includes necessary hazard analysis, design drawing and procedural reviews, and equipment inspections. The assessment shall incorporate the scope and techniques of the PHA, RHA, SSHA, SHA, and O&SHA to the extent necessary to assure the safe design, operation, maintenance, and support of the system. A safety compliance assessment shall:

a Identify contractual military, federal, national, international, and industry safety specifications, standards, and codes applicable to the system and document compliance of the design and procedures with these requirements.

b. Identify other military, federal, national, international, and industry safety specifications, standards, and codes applicable to the system, which are required by law or the use thereof is considered good engineering practice, and document compliance of the design and procedures with these requirements.

c. Identify and evaluate residual hazards inherent in the system or that arise from system-unique interfaces, installation, test, operation, maintenance, or support.

d. Identify necessary specialized safety design features, devices, procedures, skills, training, facilities, support requirements, and personnel protective equipment

e. Identify hazardous materials and provide justification for using such a material instead of a less or non hazardous material, and the precautions and procedures necessary for safe storage, handling, transport, use, and disposal of tbe material.

402.3 **DETAILS TO BE SPECIFIED.**

402.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Tasks 101 and 402.

b. Identify applicable requirements.

THIS PAGE **INTENTIONALLY LEFT BLANK**

TASK 403

EXPLOSIVE HAZARD CLASSIFICATION AND CHARACTERISTICS DATA

403.1 PURPOSE. The purpose of this task is to require the contractor to perform those tests and procedures necessary for the explosive hazard classification(EHC) of, and for development of hazard characteristics data about, new or modified ammunition, explosives (including solid pmpellants), and devices containing explosives.

403.2 TASK DESCRIPTION.

403.2.1 Explosive hazard classification. The contractor shall perform the following tasks to support obtaining interim and/or final DOD explosive hazard classifications (EHC) for any new or modified items of ammunition or of an explosive nature that will be transported to or stored at a DOD installation or facility. The data provided will consider the explosive items shipping and storage configuration.

403.2.1.1 Interim classification by testing shall be supported by test data of the DOD Explosive Hazard Classification Procedures (DEHCP)(Air Force TO 11A-1-47, Army TB 700-2, Navy NAVSEAINST 8020.8, and DLAR 8220.1). An exception is that testing is not required for devices containing explosives/propellants listed in Title 49, CFR, Part 172, Hazardous Materials Table.

403.2.1.2 Interim classification by analogy to an item having a valid final hazard classification shall be supported by test data on the analogous item except for 1.4S items which require testing. A narrative discussing the similarities between the two devices is also required.

403.2.1.3 Final classification by testing shall be supported by the test date required in the DEHCP, paragraph 5-2 and 5-3, or in an alternative test plan proposed by the contractor and approved by the Department of Defense Explosives Safety Board through appropriate Government channels. A narrative discussing the similarities between the two devices is also required.

403.2.1.4 Final classification by analogy to a previously classified item shall be supported by the test data used to classify the analogous item except for 1.45 items which require testing.

403.2.1.5 Tbe contractor shall request renewal of an interim EHC prior to the one year anniversary of the date the last interim EHC was issued. A new interim will be required for any changes in the explosive item, shipping configuration or part number. A final EHC will be requested based upon data obtained by conducting testing required by the explosive hazard classification procedures or approved alternative test plan. The final EHC testing must be conducted on production level designed items.

403.2.2 Classifications/Markings. The contractor shall recommend a category for each item of explosives/ammunition in each of the following areas.

a. DOD Hazard Class/Division/Storage Compatibility Group (SCG).

b. Proper shipping name and United Nations number.

c. DOT Hazard Class.

d. DOT Label.

e. National Stock Number. If not available, then part number.

403.2.3 Hazard characteristics data. The contractor shall establish this data by generating or compiling sufficient safety data to reveal hazards involved in handling, shipping, and storage related to the production, procurement, and disposal of a new or modified items of ammunition or explosives.

403.2.4 Illustrations. The contractor shall prepare illustrations of the explosive part and an illustration that shows the relationship of the explosive part to the other items in the assembly. An illustration shall be prepared to show the relationship of the explosive assembly to the next higher assembly.

403.2.4 Changes. Any changes to an item that has received final hazard classification shall be reported through the Government and Industry Data Exchange Program (GIDEP) using the "PRODUCT CHANGE NOTICE" form.

403.2.5 Alternative EHC Test Plan. When directed by the MA or whenever the contractor will not follow the test procedures specified in the DOD Explosive Hazard Classification Procedures, the contractor shall develop an alternative test plan which must be approved by the MA and the DOD Explosive Safety Board before testing is conducted.

403.3 DETAILS TO BE SPECIFIED.

403.3.1 Details to be specified in the SOW shall include the following, as applicable:

(R) a. Imposition of Task 403.

(R) b. Those sections of the Department of Defense Explosives Hazard Classification Procedures containing the required test methods and procedures.

c. Specific hazard characterization data required.

TASK 404

EXPLOSIVE ORDNANCE DISPOSAL SOURCE DATA

404.1 PURPOSE. The purpose of **this task is to require the contractor to provide source data, explosive ordnance disposal procedures, recommended render safe** procedures, **and** test items for new or modified weapons systems, explosive ordnance items, and aircraft systems.

404.2 TASK DESCRIPTION.

404.2.1 Source Data The **contractor shall** provide detailed source data on explosive ordnance design functioning, and safety so that proper EOD tools, equipment and procedures can be validated and **verified.** The Naval Explosive Ordnance Disposal Technology Center **(NAVEODTECHCEN),** Indian Head, MD. will assist in establishing quantities and types of assets required.

404.22 Explosive ordnance disposal procedures. **The** contractor shall provide courses of action to be taken by explosive ordnance disposal personnel to render safe and dispose of explosive ordnance.

404.2.3 Test items. The contractor **shall** provide test ordnance for the conduct of EOD validation and verification testing.

404.3 DETAILS TO BE SPECIFIED.

404.3.1 Details to be specified in the SOW shall **include the following, as applicable.**

(R) a. Imposition of this Task 404

b. **Hazard** classification data for all explosive components.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

GUIDANCE FOR IMPLEMENTATION OF SYSTEM SAFETY PROGRAM REQUIREMENTS

SPECIAL ADVICE FOR THE PROGRAM MANAGER

You, the Program Manager (PM), should be aware that the issue of safety creates several conflicting incentives for contractors. Naturally, contractors have an incentive to avoid serious, flagrant hazards that may jeopardize the ultimate future of the program or **cause** them to **incur** liability for **subsequent accidents. However, through the Engineering Change Proposal (ECP) process, contractors generally benefit from hazards allowed to creep into designs. ECPs are major profit centers. The** most **difficult ECPs** for a PM to disapprove are those flagged "Safety." And if safety problems are allowed to be created and **remain** undetected until late in development, **the** fixes can wreak havoc with your budgets and schedules.

You acquire acceptably safe systems through a three step process. **First,** you need to prevent tbe initial creation **of unnecessary hazards.** You do this by communicating to the developer **that** safety is **IMPORTANT to you** personally. Insist they design it in, not add it on. **Direct** the **developer (contractor) to sensitize design engineers to be attentive to system hazards while creating the design, so they may minimize the number and severity of hazards initially residing in the system. This first step has historically** proven **to** be a significant cost and problem avoidance technique-one usually overlooked by **PMs.**

Next, carefully tailor a system safety activity to meet specific program needs. **NOTE:** If you omit the above first step, you will need a larger system safety effort to address the greater number and variety of hazards that will populate the design.

Lastly, you need to manage residual hazards. You do this by understanding their nature and impact, and assuring they are properly dispositioned. For hazards that are to be "accepted," take care to assure that this acceptance of risk occurs at **the** proper level of authority--generally the greater the risk, the higher the approval level needed for acceptance. Note that the higher level risks must be justified to **the** decision makers, not the Safety community.

10. GENERAL. System safety engineering is the element of systems engineering involving the application of scientific and engineering principles for the timely identification of hazards and initiation of the actions necessary to eliminate/control hazards or reduce the associated risk **to** an acceptable level within the system. It draws upon professional knowledge and specialized skills in the mathematical, physical, and related scientific disciplines, together with the principles and methods of engineering design and analysis to specify, predict, and evaluate the safety of the system. **The** degree of safety achieved in a system is directly dependent upon the emphasis given. **This** emphasis must be applied by the Government and contractors during all phases **of the** life cycle. Design safety is a prelude **to** operational safety and the goal is to produce au inherently safe product that will have the minimum operational safety requirements or restrictions.

10.1 Scope. **This** appendix provides rationale and guidance for the selection of requirements and tasks to fit the needs of any system safety program, and identifies applicable data items for

documenting the results of required tasks.

10.2 Purpose (Reference Paragraph 1.1). Provision for a system safety program as defined by this standard shall he included in all applicable contracts negotiated by DOD. These contracts include those negotiated within each DOD agency, by one DOD agency for another, and by DOD for other Government agencies. In addition, each DOD in-house program shall conduct a system safety program. This appendix is to he used to tailor system safety requirements in the most cost effective manner that meets established program objectives. However, it is not intended to he referenced or implemented iu contractual documents

10.3 User. The user of this appendix may include the DOD MA, Government in-house activity, prime contractors, associate contractors, or subcontractors, who wish to impose system safety tasks upon their supplier(s).

10.4 Contractual Requirements. This standard shall he tailored and incorporated in the list of compliance documents. Tailored system safety program requirements are specified in the contractual provisions including the SOW, bidders' iustructious, contract data requirements list, general and special provision sections, annexes, and other contract4 means. A draft SSPP may be submitted with the contractor's proposal and be subject to contract negotiation. Upon approval by the MA, this SSPP should be attached to the contract, referenced in the SOW, and with applicable portions of this standard become the basis for contractual requirements.

10.5 Managing Activity Responsibilities. The MA will:

a Establish, plan, organize, implement and maintain an effective system safety program that is integrated iuto all life cycle phases.

b. Establish definitive system safety program requirements for the procurement or development of a system. The requirements shall be set forth clearly in the appropriate system specifications and contractual documents and define:

(1) In the appropriate system specifications, the system safety design requirements that are available and applicable, and the specific risk levels considered acceptable for the system Acceptable risk levels will be defined in terms of: a hazard risk index developed through a hazard severity/hazard probability matrix; an overall system mishap rate; demonstration of controls required to preclude unacceptable conditions; satisfaction of specified standards/regulatory requirements; or other suitable risk assessment procedures.

(2) In the SOW, the system safety requirements that cannot be defined in the system specifications. This would include general design guidelines in paragraph 4.3.

(3) In the SOW and contract data requirements list as applicable, the specified safety data; e.g., analyses, tests, or progress reports that will be required during the scope of the effort

c. Ensure that an SSPP is prepared that reflects in detail how the total program is to be conducted.

d. Review and approve for implementation the SSPPs prepared by the contractor.

e. Supply historical safety data as available.

f. Monitor contractors' system safety activities and review and approve deliverable data, if applicable, to ensure adequate performance and compliance with system safety requirements.

g. Ensure that the appropriate system specifications are updated to reflect results of analyses, tests, and evaluations.

h. Evaluate new design criteria for inclusion into military specifications and standards and submit recommendations to the respective responsible organization.

i. Establish system safety groups as required by the appropriate service organizations to assist the program manager in developing and implementing a system safety program.

j. Establish work breakdown structure elements at appropriate levels for system safety program management and engineering.

k. Provide technical data on GFE/GFP to enable the contractor to accomplish the defined tasks.

20. REFERENCED DOCUMENTS. Referenced documents are not included herein. Referenced documents required to supplement this military standard are specified in the system specifications and other contractual documents.

30. SYSTEM SAFETY REQUIREMENTS. Section 4, "General Requirements", provides basic system safety requirements most DOD systems and facilities acquisition programs should meet. Task 101, which implements Section 4, mast he imposed as a single general task to instruct the contractor to conduct a system safety program. It can be tailored to fit the different types and sizes of programs. Additional tasks in section 100, 200, 300 and 400 or other specific tasks not in this standard, must also he detailed in the SOW to fulfill specific needs of individual programs.

30.1 System safety program (Reference paragraph 4.1). The MA must make sure that the contractor has a viable system safety program. This paragraph directs the establishment of such a program and, if tasked, the SSPP will describe it

30.1.1 Management system. Whether the contractor ha5 an existing system safety management structure or has to create one, the MA needs to examine the policies and processes to determine if they are consistent with program requirements. The MA shall then attempt to resolve any such issues promptly to avoid program delays or disconnects. The MA should also specify any special incident investigation and reporting requirements.

30.1.2 Key system safety personnel. The MA can require that key system safety personnel meet certain minimum qualifications. Key system safety personnel are usually limited to the person who has supervisory responsibility/technical approval authority for the system safety work. A guide is provided at Table 3. The MA must specify the minimum qualifications of key personnel in the SOW. Some programs will require that key system safety personnel possess special qualifications. These special qualifications must also he specified in the SOW.

TABLE 3. MINIMUM QUALIFICATIONS FOR KEY SYSTEM SAFETYPERSONNEL

Program Complexity	Education	Experience	Certification
High	BS in Engineering, Physical Science or other*	Four years in system safety or related discipline	Desired: CSP# or Professional Engr.
Moderate	Bachelor's Degree plus training in system safety	Two years in system safety or related discipline	Enhancement: CSP# or Professional Engr.
Low	High School Diploma plus training in system safety	Four years in system safety	None

* NOTE: MA may specify other degrees or certification in SOW.
# CSP - Certified Safety Professional

3 0 2 System safety program objectives (Reference Paragraph 4.2). These are the core system safety program objectives and are applicable to most, if not all, DOD systems and facilities acquisition programs. The MA may add to, delete or modify these objectives to fit the project.

3 0 . 3 System Safety Design requirements (Reference Paragraph 4.3). These are the general design requirements needed to meet the core objectives. The MA must provide more specific guidance to the contractor based on the type of system being acquired. The more closely the requirements relate to a given project, the easier the designers can incorporate them into the system.

3 0 . 4 System safety precedence (Reference Paragraph 4.4).

30.4.1 The overall goal of a system safety program is to design systems that do not contain hazards which can result in an unacceptable level of mishap risk since the nature of most complex systems makes it impossible or impractical to design them completely hazard-free. As hazard analyses are performed, hazards will be identified that will require resolution System safety precedence defines the order to be followed for satisfying system safety requirements and reducing risks. The alternatives for eliminating the specific hazard or controlling its associated risk are evaluated so that an acceptable method for risk reduction can be agreed to.

30.42 Hazard identification, categorization, and corrective actions are to proceed through design, development, and testing of all development phases. Assessment of risk is necessary in determining what corrective actions are to be taken. Whatever level of hazard risk reduction is taken, it is to be thoroughly justified in all cases.

30.5 Risk assessment (Reference Paragraph 4.5).

30.51 To determine what actions to take to eliminate/control identified hazards, a system of determining the level of risk involved must be developed. A good risk assessment model will enable decision makers to properly understand the amount of risk involved relative to what it will cost in

schedule and dollars to reduce that risk to an acceptable level.

30.62 To eliminate or otherwise control as many haxards as possible, prioritize haxards for corrective action. A categorization of hazards ma.. be conducted according to risk level criteria. Categorization may be based on severity since not all hazards are of equal magnitude or criticality to personnel safety and mission success. In some cases, the anticipated consequences of hazardous events may be minimal, while in others, catastrophic. Hazard categorization may also involve the determination of the likelihood of the hazardous event actually occurring. 'Ibis may be reported in non-numeric (qualitative) terms, such as frequent, occasional, or improbable: or in numeric (quantitative) terms such as once in ten thousand flights, or $1X10^{-4}$/flight. Prioritization may be accomplished either subjectively by qualitative analyses resulting in a comparative hazard risk assessment or through quantification of the probability of occurrence resulting in a numeric priority factor for that hazardous condition. Figures 1 and 2 show two sample matrices for hazard risk assessment which can be applied to provide qualitative priority factors for assigning corrective action. In the first matrix an identified hazard assigned a hazard risk index of 1A, 1B, 1C, 2A, 2B, or 3A might require immediate corrective action. A hazard risk index of 1D, 2C, 2D, 3B, or 3C would be tracked for possible corrective action. A hazard risk index of 1E, 2E, 3D, or 3E might have a lower priority for corrective action and may not warrant any tracking actions. In the second matrix, risk indices of 1 through 20 (1 being highest risk) are assigned somewhat arbitrarily. This matrix design assigns a different index to each frequency-category pair thus avoiding the situation caused

FIGURE 1. FIRST EXAMPLE HAZARD RISK ASSESSMENT MATRIX

HAZARD CATEGORY / FREQUENCY	(1) CATASTROPHIC	(2) CRITICAL	(3) MARGINAL	(4) NEGLIGIBLE
(A) FREQUENT ($X > 10^{-1}$)*	1A	2A	3A	4A
(B) PROBABLE ($10^{-1} > X > 10^{-2}$)*	1B	2B	3B	4B
(C) OCCASIONAL ($10^{-2} > X > 10^{-3}$)*	1C	2C	3C	4C
(D) REMOTE ($10^{-3} > X > 10^{-6}$)*	1D	2D	3D	4D
(E) IMPROBABLE ($10^{-6} > X$)*	1E	2E	3E	4E

* Example of quantitative criteria

Hazard Risk Index	Suggested Criteria
1A, 1B, 1C, 2A, 2B, 3A	Unacceptable
1D, 2C, 2D, 3B, 3C	Undesirable (MA decision required)
1E,2E,3D,3E,4A,4B	Acceptable with review by MA
4C, 4D, 4E	Acceptable without review

FIGURE 2. SECOND EXAMPLE HAZARD RISK ASSESSMENT MATRIX

HAZARD CATEGORY / FREQUENCY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
FREQUENT	1	3	7	13
PROBABLE	2	5	9	16
OCCASIONAL	4	6	11	16
REMOTE		10		19
IMPROBABLE	12	15		20

Hazard Risk Index	Suggested Criteria
1 - 5	Unacceptable
6 - 9	Undesirable (MA decision required)
10-17	Acceptable with review by MA
18 - 20	Acceptable without review

by creating indices as products of numbers assigned to frequency and category which causes common results such as 2 X 6 = 3 X 4 = 4 X 3. This situation hides information pertinent to prioritization. These are only examples of a risk assessment methods and do not fit all programs. The MA working with the contractor(s) must decide the proper risk assessment approach for each system. Then describe the risk assessment method in the SSPP or other appropriate document.

30.5.3 Risk Impact. This is a means of further prioritizing hazards that may have the same risk hazard index, other factors (such as effect on mission/operation or economic, sociological and political implications to the extent known) when assessing the risk. An example is the use of a hazardous material that could contaminate the environment, cause adverse health effects to service members as well as private citizens and result in hazardous wastes that must be treated specially even if no mishap occurs. The material may deserve higher consideration for resolution than a hardware design that could cause a loss of a system through a mishap. The MA should identify any impacts they want the contractor to consider when tailoring Section 4.

30.6 Action on Identified Hazards (Reference paragraph 4.6). By this requirement the contractor is to resolve CATASTROPHIC and CRITICAL hazards through design changes or incorporation of safety devices. If the MA desires other hazards to be handled in this way, the paragraph is to be tailored to so indicate. The MA must also make sure the contractor knows how to process alternative recommendations, if needed. Usually the contractor processes these recommendations as part of a hazard analysis or hazard tracking technique. Programs that don't require one of these approaches must provide a recommendation procedure.

30.6.1 Residual Risk (Reference paragraph 4.6.1). The MA must know what residual risk exists in the system being acquired. For significant hazards, the MA is required to raise residual risk to higher levels

FIGURE 3. EXAMPLE DECISION AUTHORITY MATRIX FOR RESIDUAL RISK

HAZARD CATEGORY / FREQUENCY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
FREQUENT	HIGH	HIGH	HIGH	MEDIUM
PROBABLE	HIGH	HIGH	MEDIUM	LOW
OCCASIONAL	HIGH	HIGH	MEDIUM	LOW
REMOTE	HIGH	MEDIUM	LOW	LOW
IMPROBABLE	MEDIUM	LOW	LOW	LOW

Hazard Risk Level	Decision Authority
HIGH	Service Acquisition Executive
MEDIUM	Program Executive Officer
LOW	Program Manager

such as the Program Executive Officer or Service Acquisition Executive for action or acceptance. This requirement causes the contractor to document the action(s) taken within the scope of the contract. The MA may be able to apply additional resources or other remedies to help the contractor satisfactorily resolve the issue. If not, the MA can add their position to the contractors information, and forward the matter to a higher decision authority. Figure 3 is an example of a decision authority matrix based on the hazard risk index approach.

30.7 Software Hazard Risk Assessment Process. The initial assessment of risk for software, and consequently software controlled or software intensive systems, cannot rely solely on the hazard severity and probability. Determination of the probability of failure of a single software function is difficult at best and cannot be based on historical data. Software is generally application specific and reliability parameters associated with it cannot be estimated in the same manner as hardware is. Therefore, another approach is recommended for the initial software risk assessment that considers the potential hazard severity and the degree of control that software exercises over the hardware. The degree of control is defined using the software control categories.

a. Software Control Categories.

I Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence.

IIa Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.

IIb Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the hazard's occurrence.

IIIa Software item issues commands over potentially hazardous hardware systems,

subsystems or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.

IIIb Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.

IV Software does not control safety critical hardware systems, subsystems or components and does not provide safety critical information.

b. Software Hazard Criticality Matrix. The Software Hazard Criticality Matrix (Fig 4) is similar to the Hazard Risk Assessment Matrix in this Appendix The matrix is established using the hazard categories for the rows and the Software Control Categories for the columns. The matrix is completed by assigning Software Hazard Risk Index numbers to each element just as Hazard Risk Index numbers are assigned in the Hazard Risk Assessment Matrix. A Software Hazard Risk Index (SHRI) of '1' from the matrix implies that the risk may be unacceptable. A SHRI of '2' to '4' is undesirable or requires acceptance from the managing activity. Unlike the hardware related HRI, a low index number does not mean that a design is unacceptable. Rather, it indicates that greater resources need to be applied to the analysis and testing of the software and its interaction with the system.

FIGURE 4. EXAMPLE SOFTWARE HAZARD CRITICALITY MATRIX.

HAZARD CATEGORY / CONTROL CATEGORY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
I	1	1	3	5
II	1	2	4	5
III	2	3	5	5
IV	3	4	5	5

Hazard Risk Index	Suggested Criteria
1	High risk - significant analysis and testing resources
2	Medium risk - requirements and design analysis and in-depth testing required
3-4	Moderate risk - high level analysis and testing acceptable with Managing Activity approval
5	Low Risk - Acceptable

40. TASK SELECTION

40.1 Selection Criteria

FIGURE 3. EXAMPLE DECISION AUTHORITY MATRIX FOR RESIDUAL RISK

HAZARD CATEGORY / FREQUENCY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
FREQUENT	HIGH	HIGH	HIGH	MEDIUM
PROBABLE	HIGH	HIGH	MEDIUM	LOW
OCCASIONAL	HIGH	HIGH	MEDIUM	LOW
REMOTE	HIGH	MEDIUM	LOW	LOW
IMPROBABLE	MEDIUM	LOW	LOW	LOW

Hazard Risk Level	Decision Authority
HIGH	Service Acquisition Executive
MEDIUM	Program Executive Officer
LOW	Program Manager

such as the Program Executive Officer or Service Acquisition Executive for action or acceptance. This requirement causes the contractor to document the action(s) taken within the scope of the contract. The MA may be able to apply additional resources or other remedies to help the contractor satisfactorily resolve the issue. If not, the MA can add their position to the contractors information, and forward the matter to a higher decision authority. Figure 3 is an example of a decision authority matrix based on the hazard risk index approach.

30.7 Software Hazard Risk Assessment Process. The initial assessment of risk for software, and consequently software controlled or software intensive systems, cannot rely solely on the hazard severity and probability. Determination of the probability of failure of a single software function is difficult at best and cannot be based on historical data Software is generally application specific and reliability parameters associated with it cannot be estimated in the same manner as hardware is. Therefore, another approach is recommended for the initial software risk assessment that considers the potential hazard severity and the degree of control that s&ware exercises over the hardware. The degree of control is defined using the software control categories.

a. Software Control Categories.

I Software exercises autonomous control over potentially hazardous hardware systems, subsystems or components without the possibility of intervention to preclude the occurrence of a hazard. Failure of the software or a failure to prevent an event leads directly to a hazard's occurrence.

IIa Software exercises control over potentially hazardous hardware systems, subsystems, or components allowing time for intervention by independent safety systems to mitigate the hazard. However, these systems by themselves are not considered adequate.

IIb Software item displays information requiring immediate operator action to mitigate a hazard. Software failures will allow or fail to prevent the hazard's occurrence.

IIIa Software item issues commands over potentially hazardous hardware systems,

subsystems or components requiring human action to complete the control function. There are several, redundant, independent safety measures for each hazardous event.

IIIb Software generates information of a safety critical nature used to make safety critical decisions. There are several, redundant, independent safety measures for each hazardous event.

IV Software does not control safety critical hardware systems, subsystems or components and does not provide safety critical information.

b. Software Hazard Criticality Matrix. The Software Hazard Criticality Matrix (Fig 4) is similar to the Hazard Risk Assessment Matrix in this Appendix. The matrix is established using the hazard categories for the rows and the Software Control Categories for the columns. The matrix is completed by assigning Software Hazard Risk Index numbers to each element just as Hazard Risk Index numbers are assigned in the Hazard Risk Assessment Matrix. A Software Hazard Risk Index (SHRI) of '1' from the matrix implies that the risk may be unacceptable. A SHRI of '2' to '4' is undesirable or requires acceptance from the managing activity. Unlike the hardware related HRI, a low index number does not mean that a design is unacceptable. Rather, it indicates that greater resources need to be applied to the analysis and testing of the software and its interaction witb the system.

FIGURE 4. EXAMPLE SOFTWARE HAZARD CRITICALITY MATRIX.

HAZARD CATEGORY / CONTROL CATEGORY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
I	1	1	3	6
II	1	2	4	5
III	2	3	5	5
IV	3	4	5	5

Hazard Risk Index	Suggested Criteria
1	High risk - significant analysis and testing resources
2	Medium risk - requirements and design analysis and in-depth testing required
3-4	Moderate risk - high level analysis and testing acceptable with Managing Activity approval
5	Low Risk - Acceptable

40. TASK SELECTION

40.1 Selection Criteria

40.1.1 A major challenge which confronts all Government and industry organizations responsible for a system safety program is the selection and timing of tasks and availability of hazard analyses, which can materially aid in attaining program safety requirements. Schedule and funding constraints mandate a cost effective selection, one that is based on identified program needs. The considerations presented herein are intended to provide guidance and rationale for this selection. They are also intended to jog the memory for lessons learned to provoke questions which must be answered and to encourage dialogue with other engineers, and operations and support personnel so that answers to questions and solutions to problems can be found. Tables 4 and 5, and Appendix B provides guidance for timing of task requirements, data deliverables, and completion and availability of hazard analyses results.

40.1.2 Once appropriate tasks have been selected, the tasks themselves must be tailored and specified by the MA as outlined in the "DETAILS TO BE SPECIFIED." It is also important to coordinate task requirements with other engineering support groups, such as logistics support, reliability, etc., to eliminate duplication of tasks and to be aware of any additional information of value to system safety which these other groups can provide. Finally, the timing and depth required for each task, as well as action to be taken based on task outcome, are largely dependent on individual experience and program requirements. For these reasons, hard and fast rules are not stated

40.2 Application matrix for program phases. Tables 4 and 6 herein provide general guidance on task selection to establish an acceptable and cost effective system safety program. These tables can be used to initially identify those tasks which typically are included in an effective system safety program for the particular acquisition phase involved. The user of the document can then refer to the particular task referenced by the matrix aud determine from the detailed purpose at the beginning of the task if it is appropriate to identify as a program task. The use of this matrix for developing a system safety program is to be considered as optional guidance only and is not to be construed as covering all procurement situations. The provisions of applicable regulations must also be followed.

40.3 Task prioritization. The problem of prioritizing or establishing a baseline group from all the tasks in this document cannot be solved unless variables like system complexity, program phase, availability of funds, schedule, etc., are known. Task 101, System Safety Program, is required, and tailoring should be based on total program cost and complexity. All other tasks require Task 101 as a prerequisite.

40.3.1 Identifying and Quantifying System Safety Needs. The elements of a system safety program must be selected to meet the safety needs. These needs are identified by higher authority through directives and other documents. Identifying and quantifying these needs must be accomplished prior to the appropriate acquisition phase so that tasks and requirements commensurate with the needs may be included. The tasks and requirements which are included establish the framework for the continuing system safety dialogue between the MA and the proposing contractors, one or more of whom will ultimately be selected to develop the system.

40.32 Selecting Tasks to Fit the Needs In moat cases, the need for the tasks is self-evident. While experience plays a key role in task'selection, it should be supplemented by a more detailed study of the program. Consideration must be given to the size/dollar value of the program and the expected level of risk involved. The selection of tasks must be applicable not only to the program phase, but also to the perceived risks involved in the design and the funds available to perform the system safety effort. Table 6 provides examples of typically tailored system safety programs based

on size or project risk. Once recommendations for task applications have been determined and more detailed requirements identified, tasks and requirements *can be* prioritized and a "rough order of magnitude" estimate should be made of the time and effort required to complete each task. This information will be of considerable value in selecting the tasks which can be accomplished within schedule and funding constraints.

TABLE 4. APPLICATION MATRIX FOR SYSTEM PROGRAM DEVELOPMENT

TASK	TITLE	TASK TYPE	PROGRAM PHASE 0	I	II	III	IV
101	SYSTEM SAFETY PROGRAM	MGT	G	G	G	G	G
102	SYSTEM SAFETY PROGRAM PLAN	MGT	G	G	G	G	G
103	INTEGRATION/MANAGEMENT OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS, AND AE FIRMS	MGT	S	S	S	S	S
104	SYSTEM SAFETY PROGRAM REVIEW/AUDITS	MGT	S	S	S	S	S
105	SSG/SSWG SUPPORT	MGT	G	G	G	G	G
106	HAZARD TRACKING AND RISK RESOLUTION	MGT	S	G	G	G	G
107	SYSTEM SAFETY PROGRESS SUMMARY	MGT	S	G	G	G	G
201	PRELIMINARY HAZARD LIST	ENG	G	S	S	S	N/A
202	PRELIMINARY HAZARD ANALYSIS	ENG	G	G	G	GC	GC
203	SAFETY REQUIREMENTS/ CRITERIA ANALYSIS	ENG	G	S	S	S	GC
204	SUBSYSTEM HAZARD ANALYSIS	ENG	N/A	G	G	GC	GC
205	SYSTEM HAZARD ANALYSIS	ENG	N/A	G	G	GC	GC
206	OPERATING AND SUPPORT HAZARD ANALYSIS	ENG	S	G	G	GC	GC
207	HEALTH HAZARD ASSESSMENT	ENG	G	G	G	GC	GC
301	SAFETY ASSESSMENT	ENG	S	S	S	s	S
302	TEST AND EVALUATION SAFETY	ENG	G	G	G	G	G
303	SAFETY REVIEW OF ENGINEERING CHANGE PROPOSALS, SPECIFICATION CHANGE NOTICES, SOFTWARE PROBLEM REPORTS, AND REQUESTS FOR DEVIATION/WAIVER	ENG	N/A	G	G	G	G
401	SAFETY VERIFICATION	ENG	S		G	G	S
402	SAFETY COMPLIANCE ASSESSMENT	ENG	S	G	G	S	S
403	EXPLOSIVE HAZARD CLASSIFICATION AND CHARACTERISTICS DATA	MGT	S	S	S	S	S
404	EXPLOSIVE ORDNANCE DISPOSAL SOURCE DATA	MGT	S	S	S	S	S

NOTES:
TASK TYPE
ENG - System Safety Engineering
MGT - System Safety Management

PROGRAM PHASE
0 - Concept exploration
I - Demonstration/validation
II - Engineering/manufacturing Development
III - Production/deployment
IV - Operations/support

APPLICABILITY CODES
S - Selectively Applicable
G - Generally Applicable
GC - General Applicable to Design Change Only
N/A - Not Applicable

TABLE 5. **APPLICATION** MATRIXFOR **FACILITIES** ACQUISITION

TASK	TITLE	TASK TYPE	PROGRAM PHASE I	II	III	IV
101	SYSTEM SAFETY PROGRAM	MGT	G	G	G	G
102	SYSTEM SAFETY PROGRAM PLAN	MGT	S	G	G	S
103	INTEGRATION/MANAGEMENT OF ASSOCIATE CONTRACTORS, SUBCONTRACTORS, AND AE FIRMS	MGT	S	S	S	S
104	SYSTEM SAFETY PROGRAM REVIEWS/AUDITS	MGT	G	G	G	G
105	SSG/SSWG SUPPORT	MGT	G	G	G	G
106	HAZARD TRACKING AND RISK RESOLUTION	MGT	G	G	G	G
107	SYSTEM SAFETY PROGRESS SUMMARY	MGT	S	S	S	S
201	PRELIMINARY HAZARD LIST	ENG	G	N/A	N/A	S
202	PRELIMINARY HAZARD ANALYSIS	ENG	G	S	N/A	S
203	SAFETY REQUIREMENTS/CRITERIA ANALYSIS	ENG	G	S	S	GC
204	SUBSYSTEM HAZARD ANALYSIS	ENG	N/A	S	G	GC
205	SYSTEM HAZARD ANALYSIS	ENG	N/A	G	G	GC
206	OPERATING AND SUPPORT HAZARD ANALYSIS	ENG	S	G	G	GC
207	HEALTH HAZARD ASSESSMENT	ENG	G	S	N/A	N/A
301	SAFETY ASSESSMENT	ENG	N/A	S	G	S
302	TEST AND EVALUATION SAFETY	ENG	G	G	G	G
303	SAFETY REVIEW OF ECPS, SPEC CHANGE NOTICES, SOFTWARE PROBLEM REPORTS, AND REQUESTS FOR DEVIATION/WAIVER	ENG	S	S	S	S
401	SAFETY VERIFICATION	ENG	N/A	S	S	S
402	SAFETY COMPLIANCE ASSESSMENT	MGT	N/A	S	S	S
403	EXPLOSIVE HAZARD CLASSIFICATION AND CHARACTERISTICS DATA	ENG	WA	S	S	S
404	EXPLOSIVE ORDNANCE DISPOSAL SOURCE DATA	MGT	N/A	N/A	S	S	S

NOTES: TASK TYPE
ENC - System Safety Engineering
MGT - System Safety Management

PROGRAM PHASE
I - Programming and Requirements Development
II - Concept Design
III - Final Design
IV - Construction

APPLICABILITY CODES
S - Selectively Applicable
G - Generally Applicable
GC - General Applicable to Design Change Only
N/A - Not Applicable

TABLE 6. EXAMPLE TASK SELECTION FOR TYPICAL PROGRAMS BASED ON DOLLAR OR RISK AMOUNTS*

Small Dollar or Low Risk Program	Medium Dollar or Average Risk Program	Large Dollar or High Risk Program
TASK 101 - System Safety Program TASK 102 - SSPP TASK 201 - Preliminary Hazard List TASK 202 - PHA TASK 205 - SHA TASK 301 - Safety Assessment	TASK 101 - System Safety Program TASK 102 - SSPP TASK 104 - Reviews/ Audits TASK 105 - SSG/SSWG TASK 106 - Hazard Tracking TASK 201 - Preliminary Hazard List TASK 202 - PHA TASK 204 - SSHA TASK 205 - SHA TASK 206 - O&SHA TASK 207 - HHA TASK 402 - Safety Compliance Assessment	TASK 101 - System Safety Program TASK 102 - SSPP TASK 103 - Integration/Mgmt of Contractors TASK 104 - Reviews/Audits TASK 106 - SSG/SSWG TASK 106 - Hazard Tracking TASK 107 - Safety Progress Reports TASK 201 - Preliminary Hazard List TASK 202 - PHA TASK 204 - SSHA TASK 205 - SHA TASK 206 - O&SHA TASK 207 - HHA TASK 301 - Safety Assessment TASK 302 - Test and Eval Safety TASK 303 - Safety ECPs TASK 401 - Safety Verification TASK 403 - Explosive Hazard Class

NOTES:
(1) Each selected task is to be tailored and MA details added in the SOW.
(2) These tasks may be applied at different phases of the program (See Tables 4 & 5).

50. RATIONALE AND GUIDANCE FOR TASK SELECTIONS.

50.1 Task Section 100 - Program Management and Control.

50.1.1 System Safety Program (Task 101). This task is required if this standard is imposed. Task 101 requires the contractor to set up and conduct a system safety program to meet the requirements of Section 4. Because of the general nature of Section 4, careful tailoring of the requirements contained therein is necessary for each program, particularly for relatively small efforts.

50.1.1.1 Requirements that are not included in Section 4, such as Appendix B through D or from some source other than this standard, may be added by the MA

50.1.1.2 In this task the acceptable level(s) of risk must be specified and these levels should apply to the entire program. The MA may use one of the examples at Figures 1 or 2 or require some other approach to rank hazards. Note that the definitions of each severity and probability level should be tailored to the program and not left so generic.

50.1.1.3 If the MA has specific requirements for handling incidents and wants the contractor to adhere to these requirements, this is a good place to insert them. Also, other items such as those

listed in paragraph 101.3.1.e should be included.

50.1.2 System Safety Program Plan (Task 102).

50.1.2.1 The system safety program plan (SSPP) is a basic tool used by the MA to assist in managing an effective system safety program. It can be used to evaluate the various contractors' approaches to, understanding of, and execution of their system safety tasks, their depth of planning to make sure their procedures far implementing and controlling system safety tasks are adequate, and their organizational structure to make sure appropriate attention will be focused on system safety activities.

50.1.2.2 A SSPP is normally prepared by the contractor and when approved by the MA, becomes the basis of understanding between the contractor and the MA as to how the system safety program is to be conducted. The approved SSPP may serve as a contractually binding document vice a guidance document. The MA must place 8 requirement for this in the SOW.

50.1.2.3 The SSPP identifies all safety program activities specified by the MA and shows how the safety program will provide input or preclude duplication of effort. The plan provides specific information to show how the contractor will meet quantitative and/or qualitative safety requirements during development, production, and construction phases. When prepared in response to a request for proposal, the SSPP serves as a thorough cross-index to the safety management and engineering proposals contained in the contractor's response. This plan must clearly reflect the safety features of the response.

50.1.24 On small programs, or large programs with several associate contractors where the MA is the integrator, or where the MA has a firm idea of the type and magnitude of the system safety effort required, the MA may prepare the SSPP and attach it to the SOW. This often will save funds since the MA would not need to buy the plan from the contractor, and also informs the contractor just what is expected. Not only does this allow contractors to price the effort in their bids, it eliminates the possibility of entering into multiple rounds of submittals and disapprovals due to miscommunication on both sides as to what is desired. However, if the contractor does not prepare an SSPP, other than in the proposal itself, the MA obtains no immediate information as to whether the contractor understands the system safety requirements. Even with an MA prepared SSPP some data must be provided by the contractor to describe particular contractor organization and internal processes and interfaces. Some MA's have developed "fill-in-the-blank" SSPPs to simplify and standardize contractor responses and responsibilities.

50.1.2.5 The format and instructions for preparing an SSPP are specified in Task 102 and DOD authorized Data Item DI-SAFT-80100A, System Safety Program Plan. This date item must be tailored for each program by requiring certain paragraphs to be listed on the contract data requirements list, DD Form 1423. Preliminary SSPPs are often required to be submitted with the contractor's proposal. This allows for the proposed system safety effort to be considered during source selection. Additionally, if the scope of the effort is excessive, inadequate, or misdirected, it provides time to get the contractor or MA to resolve the issues and revise the SSPP prior to contract initiation.

50.1.3 Integration/Management of Associate Contractors, Subcontractors and Architect and Engineering Firms (Task 103). Major programs or construction projects will often have an integrating contractor, multiple associate contractors and subcontractors, and AE firms under contract. An integrating contractor or a facilities acquisition contractor will often have the responsibility to oversee system safety efforts of associate contractors or AE firms. Task 103

provides the authority for management surveillance needed by the integrating or facilities acquisition contractor by assigning the various system safety roles of associate contractors, subcontractors, integrators, and construction firma The integrator should be tasked to write an ISSPP according to the requirements outlined in Task 102. The integrator or facilities acquisition contractor should be tasked to perform system hazard analyses and assessments to cover the interfaces between the various contractors' portions of the system or construction effort. All contractors and AE firms should be made aware of the integrator's or facilities acquisition contractor's role of overall system safety management The integrator needs to resolve differences between associates in safety-related areas. The MA will aid the integrator in these efforts to make sure all contractors and firms mutually understand the system safety requirements, and their respective responsibilities to comply with them.

50.1.4 System Safety Program Reviews/Audits (Task 104).

50.141 In addition to the system safety reviews required by other DOD or service regulations and MIL-STDs (at milestone design reviews and audits), the MA may require special safety reviews or audits. Note that the first subtask is for contractor performed reviews/audits, and the second subtask is for contractor support of reviewdaudits performed by the MA on the contractor(s). Early in a major program, system safety reviews should be held at least quarterly and as the program progresses, time between reviews can be extended. In addition to more detailed coverage of those items discussed at milestone design reviews, the reviews should address progress on all system safety tasks specified in the SOW.

50.1.4.2 All program reviews/audits provide an opportunity to review and assign action items and to explore other areas of concern. A mutually acceptable agenda/checklist should be written to make sure all system safety open items are covered and that all participants are prepared for meaningful discussions. It may be cost effective to specify that these system safety reviews/audits be held in conjunction with Program Management Review or System Safety Group meetings; however, care must be taken to provide adequate time and attention to the review or audit.

50.1.4.3 Contractor support of special system safety reviews may be needed to fulfill requirements of phase safety reviews, munitions safety boards, flight readiness reviews, and other safety review/certification authorities. Support requirements should be specified in the SOW as part of Task 104. The MA should provide as much detail on the who, what, when, where, and why for each special review process so that the contractor can properly price the effort DI-SAFT-80105A, System Safety Program Progress Report, can be used to document reviews/audits.

50.1.5 System Safety Group/System Safety Working Group Support (Task 105).

50.1.6.1 Individual service regulations require formation of SSG/SSWGs for acquisition of expensive, complex or critical systems, equipment or major facilities. Contractor support of an SSG/SSWG is very useful and may be necessary to make sure procured hardware and software is acceptably free from hazards that could injure personnel or cause unnecessary damage or loss. The level of support desired from the contractor must be detailed in the contract through imposition of Task 105.

50.1.5.2 A minimum of one SSG meeting per year is recommended. Specify the roles of the contractor(s) and planned locations of the SSG meetings. Holding some at the contractor's plant allows more participation by the contractor's staff and a chance for everyone to see the developing system.

50.1.6 Hazard Tracking and Risk Resolution (Task 106). A method or procedure must be developed to document and track hazards and progress made toward elimination or control of hazards and reduction of the associated risk. Each prime or associate contractor may maintain their own hazard log or assessment report, or the integrator or MA will maintain the document. If the contractor is to maintain the log, Task 106 must be imposed. Each hazard that meets or exceeds the threshold specified by the MA shall be entered on the log when first identified, and each action taken to eliminate the hazard or reduce the associated risk thoroughly documented. The MA will detail the procedure for closing-out the hazard, or acceptance of any residual risk. The hazard log may be documented and delivered as part of the system safety progress summary using DI-SAFT-80105A, System Safety Program Progress Report, or it can be included as part of an overall program engineering/management report.

50.1.7 System Safety Progress Summary (Task 107). The system safety progress summary provides a periodic written report of the status of system safety engineering and management activities. This status report may be submitted monthly or quarterly. It can be formatted and delivered according to DI-SAFT- 80105A, System Safety Program Progress Report, or it can be included as part of an overall program engineering/management report

50.2 Task Section 200 - Design and Integration.

50.2.1 Preliminary Hazard List (Task 201). The PHL provides to the MA a list of hazards that may require special safety design emphasis or hazardous areas where in-depth analyses need to be done. The PHL may be required as part of the bidder's response to an RFP. The MA may use the results of the PHL to determine hazards associated with the proposed concept, system safety capability of the contractor, or the scope of follow-on hazard analyses (PHA, SSHA, etc.). The PHL may be obtained using DI-SAFT-80101A, System Safety Hazard Analysis Report

50.2.2 Preliminary Hazard Analysis (Task 202).

50.2.2.1 PHA is, as implied by the title, the initial effort in hazard analysis during the system design phase or the programming and requirements development phase for facilities acquisition. It may also be used on an operational system for the initial examination of the state of safety. The purpose of the PHA is not to affect control of all risks but to fully recognize the hazardous states with all of the accompanying system implications.

50.2.2.2 The PHA effort should be commenced during the initial phases of system concept, or in the case of a fully operational system, at the initiation of a safety evaluation. This will help in the use of PHA results in tradeoff studies which are so important in the early phases of system development or, in the case of an operational system, aid in an early determination of the state of safety. The output of the PHA may be used in developing system safety requirements and in preparing performance and design specifications. In addition, the PHA is the basic hazard analysis which establishes the framework for other hazard analyses which may be performed.

50.2.2.3 The PHA should include, but not be limited to, the following activities:

a A review of pertinent historical safety experience.

b. A categorized listing of known hazards.

c. An investigation of the various hazards to determine the provisions which have been developed for their control.

d. Identification of the safety requirements and other regulations pertaining to personnel safety, environmental hazards, and toxic substances with which the system will have to comply.

e. Recommend corrective actions.

50.2.2.4 Since the PHA should be initiated very early in the planning phase, the data available to the analyst may be incomplete and informal. Therefore, structure the analysis to permit continual revision and updating as the conceptual approach is modified and refined As soon as the subsystem design details are complete enough to allow the analyst to begin the subsystem hazard analysis in detail, terminate the PHA. Provide the analyst performing the PHA with the following reference input information:

a Design sketches, drawings, and data describing the system and subsystem elements for the various conceptual approaches under consideration.

b. Functional flow diagrams and related data describing the proposed sequence of activities, functions, and operations, involving the system elements during the contemplated life span.

c. Background information related to safety requirements associated with the contemplated testing, manufacturing, storage, repair, and use locations and safety related experiences of similar previous programs or activities.

50.2.2.5 The techniques used to perform this analysis must be carefully selected to minimize problems in performing follow-on analyses. The PHA may be documented as outlined in DI-SAFT-80101A, System Safety Hazard Analysis Report There are several formats that can be used. Some of these are:

50.2.2.5.1 Narrative format The narrative format is relatively unstructured and as a result there are many different formats available. The format primarily depends on the analyst and the type of information required from the analysis.

50.2.2.5.2 Matrix format. The matrix format (also called tabular or columnar1 is the most commonly used approach for performing and documenting a PHA There are numerous varieties of PHA matrix formats in use, most of which are fairly similar.

50.2.2.5.3 Other formats. The format used should be tailored to reflect the nature of the system to be analyzed, the extent of information about the system, and the planned use of the analysis output data. The analyst must determine which can do the job most effectively. The use of system safety design checklists, such as Air Force Materiel Command Design Handbook 1-X, in the performance of a PHA can be a very effective method.

50.2.3 Safety Requirements/Criteria Analysis (Task 203). In the early system design phase, the contractor shall anticipate the system design, including likely software control and monitoring functions, safing systems, etc., to determine the potential relationship between system level hazards, hardware elements and software control, monitoring and safety functions. From this analysis, the contractor shall develop design requirements, guidelines and recommendations to eliminate or reduce the risk of those hazards to an acceptable level. In addition, generic

requirements documents shall be examined and the applicability of the design requirements determined and included in the analysis. During the system requirements analysis and functional allocation phases, the contractor shall analyze the system and software design and requirements documents to refine the identification of potential hazards associated with the control of the system, safety critical data generated or controlled by the system, safety critical non-control functions performed by the system, and unsafe operating modes for resolution. The Safety Requirements/ Criteria Analysis is substantially complete by the time the allocated baseline is defined. The requirements are developed to address hazards, both specific and non-specific, in hardware and software. While the development of requirements is generally intended to be part of the PHA, often this aspect is not accomplished and the SRCA is directed specifically at this. In addition, the PHA does not lend itself to the inclusion of design requirements that are not related to an identified hazard. The SRCA can be documented using DI-SAFT-80101A, System Safety Hazard Analysis Report.

50.2.3.1 The MA must define acceptable levels of risk; however, if this has been defined in tailoring another task for the program, it is not necessary to repeat it here.

5023.2 The MA must provide the who, what, when, and where of the review support required.

50.2.3.3 The MA may require the we of more than one type of hazard assessment particularly when examining software requirements.

50.2.4 Subsystem Hazard Analysis (Task 204).

50.2.4-l Tbis task would be performed if a system under development contained subsystems or components that when integrated functioned together as a system. Tbis analysis looks at each subsystem or component and identifies hazards associated with operating or failure modes and is especially intended to determine how operation or failure of components affects the overall safety of the system. This analysis should identify necessary actions, using the system safety precedence to determine how to eliminate or reduce the risk of identified hazards.

50.2.4.2 As soon as subsystems are designed in sufficient detail, or well into concept design for facilities acquisition, the SSHA can begin. It should be updated as the design matures. Design changes to components will also need to be evaluated to determine whether the safety of the system is affected. Tbe techniques used for this analysis must he carefully selected to minimize problems in integrating subsystem hazard analyses into the system hazard analysis. The SSHA may be documented as outlined in DI-SAFT-80101A, System Safety Hazard Analysis Report

50.2.5 System Hazard Analysis (Task 205).

50.2.5.1 A SHA is accomplished in much the same way as the subsystem hazard analysis. However, as the SSHA examines how component operation or failure affects the system, the SHA determines how system operation and failure modes can affect the safety of the system and its subsystems. The SHA should begin as the system design matures, around the preliminary design review or the facilities concept design review milestone, and should be updated until the design is complete. Design changes will need to be evaluated to determine their effects on the safety of the system and its subsystems. This analysis should contain recommended actions, applying the system safety precedence, to eliminate or reduce the risk of identified hazards.

50.2.5.2 Specifically, the SHA examines all subsystem interfaces and interfaces with other systems for:

a. Compliance with safety criteria called out in the applicable system/subsystem requirements documents.

b. Possible combinations of independent or dependent failures that can cause hazards to the system or personnel. Failures of controls and safety devices should be considered.

c. How normal operations of systems and subsystems can degrade the safety of the system.

d. Design changes to system, subsystems, or interfaces, logic, and software that can create new hazards to equipment and personnel.

The techniques used to perform this analysis must be carefully selected to minimize problems in integrating the SHA with other hazard analyses. The SHA may be documented as outlined in DI-SAFT-80101A, System Safety Hazard Analysis Report.

50.2.6 Operating and Support Hazard Analysis (O&SHA) (Task 206).

50.2.6.1 The O&SHA is performed primarily to identify and evaluate hazards associated with the environment, personnel, procedures, and equipment involved throughout the operation of a system/element. The O&SHA may be performed on such activities as testing, installation, modification, maintenance, support, transportation, ground servicing, storage, operations, emergency escape, egress, rescue, post-accident responses, and training. The O&SHA may also be selectively applied to facilities acquisition projects to make sure operation and maintenance manuals properly address safety and health requirements.

50.2.6.2 The O&SHA effort should start early enough to provide inputs to the design and prior to system test and operation. The O&SHA is most effective as a continuing closed-loop iterative process, whereby proposed changes, additions, and formulation of functional activities are evaluated for safety considerations, prior to formal acceptance. The analyst performing the O&SHA should have available:

a. Engineering descriptions of the proposed system, support equipment and facilities.

b. Draft procedures and preliminary operating manuals.

c. PHA, SSHA, and SHA reports.

d. Related requirements, constraint requirements, and personnel capabilities.

e. Human factors engineering data and reports.

f. Lessons learned, including a history of mishaps caused by human error.

50.2.6.3 Timely application of the O&SHA will provide design guidance. The findings and recommendations resulting from the O&SHA may affect the diverse functional responsibilities associated with a given program. Therefore, exercise care in assuring that the analysis results are properly distributed for the effective accomplishment of the O&SHA objectives. The techniques used to perform this analysis must be carefully selected to minimize problems in integrating O&SHAs with other hazard analyses. The O&SHA may be documented using DI-SAFT-80101~ System Safety Hazard Analysis Report

50.2.7 Tailoring of DI-SAFT-80101A. Recommended tailoring of paragraph 10.3 of the data item to include the following for each type of report required. This DID must be tailored for the specific application. The Safety Assessment Report (DI-SAFT-80102A) should be used to summarize or supplement the hazard analysis obtained under DI-SAFT-80101A. For small development programs or nondevelopmental item acquisitions, the SAR may be used as the only formal documentation of safety program activities/hazard assessment.

PARAGRAPH	PHL Task 201	PHA Task 202	SR/CA Task 203	SSHA Task 204	SHA Task 205	O&SHA Task 206
10.3.1	Yes	Yes	Yes	Yes	Yes	Yes
10.3.2	Yes	Yes	Yes	Yes	Yes	Yes
10.3.3.a	Yes	Yes	Yes	Yes	Yes	Yes
10.3.3.b(1)		Yes				
10.3.3.b(2)				Yes		
10.3.3.b(3)					Yes	
10.3.3.b(4)						Yes
10.3.3.b(5)		Yes		Yes	Yes	
10.3.3.b(6)						Yes
10.3.3.b(7)(a)	Yes	Yes				
10.3.3.b(7)(b)				Yes	Yes	Yes
10.3.3.b(8)						Yes
10.3.3.b(9)		Yes		Yes	Yes	Yes
10.3.3.b(10)		Yes		Yes	Yes	Yes
10.3.3.b(11)	Yes	Yes	Yes	Yes	Yes	Yes
10.3.3.b(12)		Yes		Yes	Yes	Yes
10.3.3.b(13)	Yes	Yes		Yes	Yes	Yes
10.3.3.b(14)		Yes		Yes	Yes	Yes
10.3.3.b(15)						Yes

SAMPLE TAILORING GUIDE

50.2.8 Health Hazard Assessment (Task 207).

50.2.8.1 The first step of the health hazard assessment (HHA) is to identify and determine quantities of potentially hazardous materials or physical agents (noise, radiation, heat stress, cold stress) involved with the system and its logistical support The next step would be to analyze how these materials or physical agents are used in the system and for its logistical support. Based on the use, quantity, and type of substance/agent, estimate where and how personnel exposures may occur and if possible the degree or frequency of exposure invoked. The final step would include incorporation into the design of the system and its logistical support equipment/facilities cost effective controls to eliminate or reduce exposures to acceptable levels. The life cycle costs of required controls could be high and consideration of alternative systems may be appropriate.

50.2.8.2 The information collected by this task will make decision authorities aware of the actual or potential health hazards of a system and their impacts so that knowledgeable decisions regarding possible tradeoffs can be made.

50.2.8.3 The following factors associated with the system and the logistical support required to operate and maintain the system should be considered:

a. Quantity, sources, nature, physical state, and toxicity and other hazards of materials.

b. Routine or planned uses and releases of hazardous materials or physical agents.

c. Accidental exposure potentials and the projected severity of those exposures.

d. Hazardous waste generated.

e. Hazardous material handling, transfer, transportation, and disposal requirements.

f. Protective clothing/equipment needs.

g. Detection and measurement devices required to quantify exposure levels.

h. Number of personnel potentially at risk.

i. Engineering controls that could be used, such as isolation, enclosure, ventilation, noise or radiation barriers, etc.

50.2.8.4 Reference quantities used in evaluating hazardous materials will include the following.

a. Acute health hazard rating based on threshold limit values (TLV), permissible exposure limits (PEL), recommended exposure limits (REL), and lethal dose (LD) limits.

b. Chronic health hazards affecting general health, reproduction, and mutagenic and tetrogenic effects.

c. Carcinogenic materials.

d. Contact hazard based on eye and skin exposure data.

e. Flammability hazards using flash point data.

f. Environmental hazards based on toxicity, ozones, organic compounds, and air quality standards.

50.2.8.5 To define the acceptable level of risk for health hazards, the MA should require use of chemical substance and physical agent, exposure limits found in appropriate regulations and directive documents, or contact a qualified health professional. For hazardous substances or agents with unspecified exposure limits the contractor must provide the rationale for acceptable risk criteria used for the HHA. The HHA may be documented using DI-SAFT-80106A, Health Hazard Assessment Report

60.3 Task Section 300 - Design Evaluation

50.3.1 Safety Assessment (Task 301). The safety assessment, a8 outlined in the task, can be written by following DI-SAFT-80102A, safety Assessment Report. The importance of this report is that it tells the user or the test team of all the residual unsafe design or operating characteristics of the system. It also attempts to quantify the risk of any hazards not eliminated, and identifies any controls, inhibits, or safety procedures. This task is also good for the evaluation of nondevelopmental items.

50.32 Test and Evaluation Safety (Task 302). This task provides needed contractor management activities to make sure all test safety requirements are met prior to and during testing. Early planning for test and evaluation must be done to consider testing milestones that will require certain hazard analyses, range or laboratory requirements that may require specially formatted assessments, review of test documents, etc.

50.3.2.1 The MA must provide the contractor information on any special system safety requirements dictated by the test or laboratory facility that will be used The MA should contact the selected range(s) and laboratory(ies) to determine and coordinate contract requirements.

50.3.2.2 The MA must identify any test and evaluation review meetings that the contractor system safety office needs to participate in or support Again, coordination with the selected facility is necessary.

50.3.2.3 Tbe MA can stipulate which hazards must be remedied. The program's hazard risk index or other risk management tool may be used to guide contractor actions. Catastrophic and critical hazards are "built into" the task, yet the MA can delete, modify or add to this requirement by tailoring the task in the SOW.

50.3.3 Safety Review of Engineering Change Proposals, Specifications Change Notices, Software Problem Reports, and Requests for Deviation/Waiver (Task 303). ECPs/SCNs/SPRs to the existing design and requests for deviation/waiver from existing requirements must be assessed for any possible safety impacts to the system. Often, correction of a deficiency will introduce other deficiencies, such as new hazards or increased risk from existing hazards, which may be overlooked. This task is designed to prevent that occurrence by requiring contractor system safety engineers to examine each ECP/SCN/SPR or request for deviation/waiver, and investigate all conceivable ways the change or deviation could result in an additional hazard(s).

50.3.3.1 The task requires that the MA be notified if the ECP/SCN/SPR or request for deviation/waiver decreases the existing level of safety. The MA should specify the criteria for determining if notification is necessary and the methodology for making notification.

50.3.3.2 The number of ECPs/SCNs/SPRs (particularly Class II) for a given program may be large. The MA can specify that the task applies to Class I changes only.

50.3.3.3 This task may be documented using DI-SAFT-80103A, Engineering Change Proposal System Safety Report, and DI-SAFT-80104A, Waiver or Deviation System Safety Report

50.4 Task Section 400 - Compliance and Verification.

50.4.1 Safety Verification (Task 401).

50.4.1.1 Many safety requirements, as specified in system specifications, requirements documents,

etc., will need to be verified by analysis, inspection, demonstration, or test. Also, during design and development, hazard analyses will identify hazards that will be removed through redesign, controls, safety devices, etc. Imposition of these changes will require verification. Task 401 outlines how safety verification should be performed.

50.4.1.2 Much of the safety verification will be outlined in system/subsystem test plans and procedures. However, for verification of risk control actions taken on hazards identified during development, special test plans/procedures will be needed. Safety tests may be documented and reported using DI-SAFT-80102A, Safety Assessment Report, or they may be included in the system/subsystem test reports.

50.4.2 Safety Compliance Assessment (Task 402).

50.4.2.1 A safety compliance assessment is conducted to verify the safe design of a system and to obtain a comprehensive evaluation of the safety risk being assumed prior to test or operation of a system. It can be documented by following DI-SAFT-80102A, Safety Assessment Report. It is an operationally oriented analysis, concerned with the safe use of a system, equipment, or facility. A safety compliance assessment is, therefore, broad in scope, covering almost every aspect of the system, but relatively general in nature, delving into detail only to the extent necessary to verify the system's safety or ascertain the risks and precautions necessary for its safe use. A safety compliance assessment may be the only analysis conducted on a program or it may serve as a pre-test or pre-operational safety review, integrating and summarizing operational safety considerations identified in more detailed hazard analyses.

50.4.2.2 A safety compliance assessment may be the only analysis conducted on a relatively low safety risk program. The low risk can result from several different factors. The system may be an integration of primarily nondevelopmental items involving little or no new design. It may be a system which is low risk by nature of its technology or complexity. Compliance with federal, military, national, and industry specifications, standards, and codes may be sufficient to make sure of the basic safety of the system. A safety compliance assessment may also be conducted on higher safety risk systems, such as research or advanced development projects, where the higher risks must be accepted, but for which safe operation is still required and the risks must be recognized and reduced to acceptable levels.

50.4.2.3 This assessment may be conducted during any phase of system development. It should be started as soon as sufficient information becomes available. For example, evaluation of equipment should begin with the design of equipment components or with the receipt of equipment specifications from a subcontractor or vendor. The analysis can also be tailored in the SOW to meet the particular needs of a program.

50.4.2.4 A safety compliance assessment should include, but not be limited to, the following

a. Identification of appropriate safety standards and verification of system compliance. Standards may be specified by the procuring agency in a specification or other contractual document. This does not preclude the contractor from identifying additional standards which are appropriate. The contractor should also review available historical safety date from similar systems. Verification may be achieved by several methods, including analysis, use of checklists, inspection, test, independent evaluation, or manufacturer's certification.

b. Analysis and resolution of system hazards. Systems, even those comprised entirely of equipment in full compliance with appropriate standards, may contain hazards resulting from

unique uses, interfaces, installation, etc. Another facet of this assessment is to identify, evaluate, and eliminate any such "residual" hazards or reduce their associated risks to acceptable levels. To accomplish this, the assessment should incorporate the scope and techniques of other hazard analyses to the detail necessary to assure a reasonably safe system. Completed analyses conducted on the system may he attached to the assessment report if so directed by the MA.

c. Identification of specialized safety requirements. The above analysis should land to safety design features and other necessary precautions. The contractor should identify all safety precautions necessary to safely operate and support the system. Thin includes applicable precautions external to the system or outside the contractor's responsibility. In order to ensure completeness of the analysis, the government must provide detailed information to the contractor on interlaces to non-contractor provided equipment. For example, hazard risk may have to be controlled by specialized safety equipment and training because the contract does not allow for redesign or modification of off-the-shelf equipment, or the contractor may not he responsible for providing necessary emergency lighting, fire protection, or personal safety equipment.

d. Identification of hazardous materials and the precautions and procedures necessary for the safe handling of the material.

50.4.3 Explosive Hazard Classification and Characteristics Data (Task 403). This task usually applies to ammunition and explosives, other than liquid explosives, in the condition and form that they are stored and offered for transportation However, it may be used to collect hazardous characteristics data for liquid propellanta.

50.4.3.1 Hazard Classification. For Department of Defense programs, the actual detailed test requirements are contained in the document entitled, "Department of Defense Explosives Hazard Classification Procedures" (Air Force TO 11A-1-47, Army TB 700- 2; Navy NAVSEAINST 8020.8, Defense Logistics Agency DLAR 8220.1). Some services may require approval of the test program by a service safety authority if it deviates from the required test series or environments. DI-SAFT-81299, Explosive Hazard Classification Data, may be used to acquire documentation from the contractor. Each organization will follow their regulations for processing the information for interim or final hazard classification The managing activity (MA) must ensure that the data requested will be sufficient to establish the interim or final hazard classification, or hazard characteristics for a production/acquisition action. Explosive hazard classification data requirements vary with each program, therefore, preparation instructions must be tailored by the contract date requirements list (CDRL) to reflect the specific requirements of the program.

50.4.3.2 Hazard Characteristics. Army organizations will require additional information on the characteristics of explosive items and should therefore use a special DID being developed by the Army to obtain this added information.

50.4.3.3 This task only asks data to be generated or compiled for new or modified ammunition or explosives. For "standard" items of ammunition or explosives, hazard characteristics are generally available. Standard items refer to commodities and related materials, components, and assemblies that have been involved in type classification or final qualification actions. Data on these standard items are not required.

50.4.3.4 The MA should contact their GIDEP representatives to assure that they will receive copies of the appropriate "PRODUCT CHANGE NOTICE" when issued.

50.4.3.5 The MA shall prepare the CDRL to require that the data package will be prepared and forwarded through the procurement agency, in sufficient copies, to arrive at the appropriate hazard classification authority at least 90 days prior to shipment of the first unit. For interim classifications, two complete copies to the Service or DLA authority (or designee) are sufficient. For final classification, six copies to the Service or DLA Headquarters authority are required.

50 4.4 **Explosive Ordnance Disposal Source Data (Task 404). This task is used to obtain** explosive ordnance disposal source data prepared in accordance with DI-SAFT-80931. The data is needed to assure that render safe procedures are obtained for the preparation of Joint Service explosive ordnance disposal technical manuals, and to develop explosive ordnance disposal response procedures to accidents/incidents that occur during testing or transportation. The data includes preliminary render safe procedures, data on hazards, functioning, and recommended tools. The Naval Explosive Ordnance Disposal Technology Center(NAVEODTECHCEN), Indian Head, MD will assist in establishing quantities and types of assets required.

50.5 **Space and Missile Data Requirements. DI-SAFT-81300,** Mishap Risk Assessment Report (MRAR), is used to consolidate, to the maximum extent possible, all hazard analyses and supporting safety data to satisfy the Missile System Prelaunch Safety Package (MSPRP) requirements of ESMCR 127-1, and the Missile System Ground Safety Approval Package (MSGSAP) requirements of WSMCR 127-l. It is mandatory for use when approval is required for operations involving the Space Transportation System (STS), or a Major Range or Test Facility Base. The MRAR certifies that all program safety requirements, including those imposed by operating site and launch vehicle agencies, have been met. Data requirements can be generated by Tasks 107, 202, 203, 204, 205, 206, 207, 301, 302, 303, 401, or 402. It will be used for the life of the program as a baseline for safety decisions involving changes to the system, operational concepts and procedures.

50.5.1 The Mishap Risk Assessment Report (MRAR) must be tailored to the specific acquisition. preparation instructions, therefore, the CDRL should specify only applicable paragraphs of this DID. The MRAR for STS is approved through the safety review process defined in SDR 127-8 Vol. I. For all other programs, approval will be in accordance with applicable contractual safety requirements. For expendable launch vehicles (ELV's) and for payloads flying on ELV's, the safety review process is defined in SDR 127-8 Vol. II.

APPENDIX B

60. SYSTEM SAFETY PROGRAM ACTIVITIES RELATED TO LIFE CYCLE PHASES.

60.1 Mission need determination. The system safety effort will support the justification for starting new major systems by identifying safety deficiencies in existing or projected capability and by identifying opportunities for system safety to improve mission capability or reduce life cycle costs.

60.2 Acquisition phases (DoDI 5000.2/Facilities).

60.2.1 Concept exploration and definition/Programming and requirements development phase. System safety tasks applicable to the concept exploration/programming and requirements development phase are those required to evaluate the alternative system concepts under consideration for development and establish the system safety programs consistent witb the identified mission needs and life cycle requirements. System safety tasks will include the following

a. Prepare an SSPP to describe the proposed integrated system safety effort for the concept exploration phase.

b. Identify applicable safety requirements documents.

c. Evaluate all considered materials, design features, maintenance, servicing, operational concepts, and environments which will affect safety throughout the life cycle. Consider hazards which may be encountered in the ultimate disposition of the entire system, or components thereof, or of dedicated support equipment, which encompasses hazardous materials and substances.

d. Perform a PHL and/or a PHA to identify hazards associated with each alternative concept.

e. Identify possible safety interface problems including problems associated with computer-controlled system functions.

f. Highlight special areas of safety consideration, such as system limitations, risks, and man-rating requirements.

g. Review safe and successful designs of similar systems for consideration in alternative concepts.

h. Define the system safety requirements based on past experience with similar systems, generic requirements documents, and preliminary safety analyses.

i. Identify any safety design analysis, test, demonstration and validation requirements.

j. Document the system safety analyses, results, and recommendations for each promising alternative system concept.

k. Prepare a summary report of the results of the system safety tasks conducted during the program initiation phase to support the decision-making process.

1. Tailor the system safety program for the subsequent phases of the life cycle and include detailed requirements in the appropriate demonstration and validation phase contractual documents.

60.22 Demonstration and validation/Concept design phase. System safety tasks during the demonstration and validation/concept design phase will be tailored to programs ranging from extensive study and analyses through hardware development to prototype testing, demonstration and validation. System safety tasks will include the following:

a. Prepare or update the SSPP to describe the proposed integrated system safety effort planned for the demonstration and validation/concept design phase.

b. Participate in tradeoff studies to reflect the impact on system safety requirements and risk. Recommend system design changes based on these studies to make sure the optimum degree of safety is achieved consistent with performance and system requirements. For munitions or systems involving explosive items, this will include explosive ordnance disposal (EOD), and demilitarization and disposal design considerations.

c. Perform or update the PHL and/or the PHA done during the concept exploration/programming and requirements development phase to evaluate the configuration to be tested. Prepare an SHA report of the test configuration considering the planned test environment and test methods.

d. Establish system safety requirements for system design and criteria for verifying that these requirements have been met. Identify the requirements for inclusion in the appropriate specifications.

e. Perform detailed hazard analyses (SSHA or SHA) of the design to assess the risk involved in test operation of the system hardware and software. Obtain and include risk assessment of other contractor's furnished equipment, of nondevelopmental, and of all interfacing and ancillary equipment to be used during system demonstration tests. Identify the need for special tests to demonstrate/evaluate safety functions.

f. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production processes and operations.

(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.

(3) Production and manufacturing control data contain required warnings, cautions, and special safety procedures.

(4) Testing and evaluation are performed to detect and correct safety deficiencies at tbe earliest opportunity.

(6) Minimum risk is involved in accepting and using new design, materials, and production and test techniques.

g. Establish analysis, inspection and test requirements for nondevelopmental items or other contractor-furnished equipment (hardware, software, and facilities) to verify that applicable system safety requirements are satisfied prior to use.

h. Perform operating and support hazard analyses of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly and/or tear-down of the test configuration. Make sure hazards identified by analyses and tests are eliminated or the associated risk is minimized. Identify the need for special tests to demonstrate or evaluate safety of test functions.

i. Review training plans and programs for adequate safety considerations.

j. Review system operation and maintenance publications for adequate safety considerations, and ensure the inclusion of applicable Occupational Safety and Health Administration (OSHA) requirements.

k. Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable US Department of Transportation (DoT), US Environmental Protection Agency (EPA), and OSHA requirements.

l. Evaluate results of safety tests, failure analyses, and mishap investigations performed during the demonstration and validation phase. Recommend redesign or other corrective action (this subparagraph does not apply to the facility concept design phase).

m. Make sure system safety requirements are incorporated into the system specification/design document based on updated system safety studies, analyses, and tests.

n. Prepare a summary report of the results of the system safety tasks conducted during the demonstration and validation/concept development phase to support the decision-making process.

o. Continue to tailor the system safety program. Prepare or update the SSPP for the full-scale engineering development phase and production phase.

p. Initiate an Operating and Support Hazard Analysis to identify any obvious hazards associated with the environment, personnel, procedures, and equipment.

q. Identify safety requirements that may require a waiver or deviation during the system life cycle.

60.2.3 Engineering and manufacturing development/Final design phase. To provide support to the system engineering program, the system safety tasks during the full-scale engineering development/final design phase will include the following:

a. Prepare or update as applicable the SSPP for the full-scale engineering development phase. Continue effective and timely implementation of the SSPP during facility final design phase.

b. Review preliminary engineering designs to make sure safety design requirement6 are incorporated and hazards identified during the earlier phases are eliminated or the associated risks reduced to an acceptable level.

c. Update system safety requirements in system specification/design documents.

d. Perform or update the SSHA, SHA and O&SHA and safety studies concurrent with the design/test effort to identify design and/or operating and support hazards. Recommend any required design change6 and control procedures.

e. Perform an O&SHA for each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, check-out, operations, foreseeable emergencies, disassembly, and/or tear-down of the test configuration. Make sure hazards identified by analyses and test6 are eliminated or their associated risk controlled. Identify the need for special tests to demonstrate or verify system safety functions. Establish analyses, inspection, and test requirement6 for other contractors' or nondevelopmental items (hardware, software, and facilities) to verify prior to use that applicable system safety requirement6 are satisfied.

f. Participate in technical design and program review6 and present results of the SSHA, SHA and/or O&SHA.

g. Identify and evaluate the effects of storage, shelf-life, packaging, transportation, handling, test, operation, and maintenance on the safety of the system and its components.

h. Evaluate result6 of safety testing, other system tests, failure analyses and mishap investigations. Recommend redesign or other corrective action.

i. Identify, evaluate, and provide safety considerations or tradeoff studies.

j. Identify safety requirement6 that may require a waiver or deviation during the system life cycle.

k. Review appropriate engineering documentation (drawings, specifications, etc.) to make sure safety consideration6 have been incorporated Also ensure that drawings for safety critical parts/items are properly marked.

l. Review logistic support publications for adequate safety considerations, and ensure the inclusion of applicable DoT, EPA, and OSHA requirements.

m. Verify the adequacy of safety and warning devices, life support equipment, and personal protective equipment.

n. Identify the need for safety training and provide safety inputs to training courses.

o. Provide system safety surveillance and support of test unit production and of planning for full-scale production and deployment. Identify critical parts aud assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the demonstration system within the production process and operations.

(2) Adequate safety provisions are included in inspections, tests, procedures, and checklists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.

(3) Production and manufacturing control data contain required warnings, cautions, and special safety procedures.

(4) Testing and evaluation are performed to detect and correct safety deficiencies at the earliest opportunity.

(5) Minimum risk is involved in accepting and using new designs, materials, and production and test techniques.

p. Make sure procedures developed for system test, maintenance, operation, and servicing provide for safe disposal of all hazardous materials. Consider any material or manufactured component (whether or not an identifiable spare part or replenishable component) when access to hazardous material will be required by personnel during planned servicing, teardown, or maintenance activities, or in reasonably foreseeable unplanned events resulting from workplace operations. Safety data developed in SSHAs, SHAs, and O&SHAs, and summarized in SARs must also identify any hazards which must be considered when the system, or components thereof, are eventually demilitarized and subject to disposal. This should include EOD requirements to render safe and dispose of explosive ordnance.

q. Prepare a summary report of the results of the system safety tasks conducted during the full-scale engineering development phase to support the decision-making process.

r. Tailor system safety program requirements for the production and deployment phase.

60.2.4 Production and deployment phase. As part of the on-going system safety program, the system safety tasks during the production and deployment phase will include the following (This paragraph is not applicable to the facilities construction life cycle. See paragraph 60.2.5):

a. Prepare or update the SSPP to reflect the system safety program requirements for the production and deployment phase.

b. Identify critical parts and assemblies, production techniques, assembly procedures, facilities, testing, and inspection requirements which may affect safety and will make sure:

(1) Adequate safety provisions are included in the planning and layout of the production line to establish safety control of the system within the production process and operations.

(2) Adequate safety provisions are included in inspections, tests, procedures, and &&lists for quality control of the equipment being manufactured so that safety achieved in design is maintained during production.

(3) Production technical manuals or manufacturing procedures contain required warnings, cautions, and special procedures.

(4) Minimum risk is involved in accepting and using new designs, materials, and production and test techniques.

c. Verify that testing and evaluation is performed on early production hardware to detect and correct safety deficiencies at the earliest opportunity.

d. Perform O&SHAs of each test, and review all test plans and procedures. Evaluate the interfaces between the test system configuration and personnel, support equipment, special test equipment, test facilities, and the test environment during assembly, checkout, operation, foreseeable emergencies, disassembly and/or tear-down of the test configuration. Make sure hazards identified by analyses and tests are eliminated or their associated risk reduced to an acceptable level.

e. Review technical data for warnings, cautions, and special procedures identified as requirements in the O&SHA for safe operation, maintenance, servicing, storage, packaging, handling, transportation and disposal.

f. Perform O&SHAs of deployment operations, and review all deployment plans and procedures Evaluate the interfaces between the system being deployed with personnel, support equipment, packaging, facilities, and the deployment environment, during transportation, storage, handling, assembly, installation, checkout, and demonstration/test operations. Make sure hazards identified by analyses are eliminated or their associated risk is reduced to an acceptable level

g. Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to make sure acceptable levels of safety are kept Identify major or critical characteristics of safety significant items that deteriorate with age, environmental conditions, or other factors.

h. Perform or update hazard analyses to identify any new hazards that may result from design changes. Make sure the safety implications of the changes are considered in all configuration control actions.

i. Evaluate results of failure analyses and mishap investigations. Recommend corrective action.

j. Monitor the system to determine the adequacy of the design, and operating, maintenance, and emergency procedures. Provide assessment/evaluation of the safety data, and recommend changes/corrective action to the MA.

k. Conduct a safety review of proposed new operating and maintenance procedures, or changes, to make sure the procedures, warnings, and cautions are adequate and inherent safety is not degraded. These reviews shall be documented as updates to the O&SHAs.

l. Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems.

m. Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety "lessons learned."

n. Evaluate the adequacy of safety and warning devices, life support equipment, and personnel protective equipment

60.2.5 Construction phase. As part of the continuing system safety program for facilities, the system safety tasks for this phase will include the following:

a Ensure the application of all relevant building safety codes including OSHA, National Fire Protection Association, U.S. Army Corps of Engineers, Naval Facilities Engineering Command, the DOD Contractors' Safety Manual for Ammunition and Explosives, and other facility related safety requirements.

b. Conduct hazard analyses to determine safety requirements at all interfaces between the facility and those systems planned for installation.

c. Review equipment installation, operation, and maintenance plans to make sure all design and procedural safety requirements have been met

d. Continue the updating of the hazard correction tracking begun during the design phases.

e. Evaluate mishap6 or other losses to determine if they were the result of safety deficiencies or oversight

f. Update hazard analyses to identify any new hazards that may result from change orders.

60.2.6 Operations and support phase. Though there is some overlap with the Production and deployment phase, the system safety tasks during this phase should be focused on a maturing system or facility that may require modifications, service life extension and, ultimately, disposal. These task include the following:

a. Evaluate results of failure analyses and mishap investigations. Recommend corrective action.

b. Update hazard analyses to reflect change6 in risk assessments, and to identify any new hazards, based on actual experience with the system or facility. Make sure the safety implications of the changes are considered in all configuration control actions.

c. Update safety documentation, such as design handbooks, military standards and specifications, to reflect safety "lessons learned."

d. Review procedures and monitor results of periodic field inspections or tests (including recall-for-tests) to make sure acceptable levels of safety are kept. Identify major or critical characteristics of safety significant items that deteriorate with age, environmental conditions, or other factors.

e. Monitor the system throughout the life cycle to determine the adequacy of the design, and operating, maintenance, and emergency procedures.

f. Document hazardous conditions and system deficiencies for development of follow-on requirements for modified or new systems.

g. Review and update disposal plans and analyses.

60.3 System safety program requirements for other acquisitions. For programs that do not follow the standard system life cycle phases outlined in the previous paragraphs, the responsible activity must carefully integrate the requirements of this standard into the acquisition process being used. Although different, facilities, ship construction, and certain major one-of-a-hind procurements still evolve through a concept/design/assembly/acceptance sequence somewhat analogous to the classic life cycle. The MA should carefully describe what system safety data are to be submitted in the appropriate contractual document, assuring these data are submitted prior to key decision points.

60.4 System safety requirements for technology development. Consider system safety during development of technology. System safety concerns should be identified and documented and guidelines developed for the technology. This documentation will provide the system safety background data necessary should a decision be made to implement the technology within a system development program.

60.5 System safety for nondevelopmental items. The procurement of a nondevelopmental item or commercial operational support or maintenance of such an item poses potential problems for the MA. These problems usually result from the fact that the item was built to commercial standards and may not satisfy every mission requirement of the procuring activity. Also, since the item already exists, the MA cannot change tbe design without greatly increasing the cost. Size of the program and planned procurement time may severely limit the scope of the system safety program and require skillful, creative tailoring of the system safety program. A small NDI program may only require the use of Tasks 101 and 301, while the MA may add Tasks 102,105 and 203 for larger programs. The following are additional NDI considerations:

60.5.1. Market investigation. It is suggested that the MA conduct a market investigation to determine, among other things, to which safety or other appropriate standards the system was designed. The MA must determine extent to which the item is certified or approved and what those certifications and approvals mean when compared to mission requirements. The following are some basic questions that should be included in any market investigation:

a. Has the system been designed and built to meet applicable/any safety standards? Request specifics.

b. Have any hazard analyses been performed? Request copies.

c. What is the mishap history for the system? Request specifics.

d. Are any protective equipment or actions needed during operation, maintenance, storage or transport of the system? Request specifics.

e. Does the system contain or use any hazardous materials (to include radioactive substances), have potentially hazardous emissions (such as from a laser), or generate hazardous waste?

f. Are special licenses *or certificates* required to own, store or use the system?

These investigations can be provided to both producers and user of the system under consideration.

60.5.2 Hazard assessment. A safety assessment (Task 301) or safety compliance assessment (Task 402) report may be all that is necessary (or available) to gather detailed hazard information concerning an NDI program. If the selected system must be modified to meet mission requirements other hazard analyses can be required. Additional analyses will be required if the NDI is going to be modified to meet military requirements not otherwise covered. The modification and its interfaces with, and the effects on or from, the item must be fully analyzed using Task 202,204 or 205. The MA may also desire a review of operation support and maintenance activities through Task 206. Hazardous materials must be addressed in the health hazard assessment (Task 207) or safety assessment (Task 301) depending on the size and complexity of the system.

60.5.3 System safety groups. Requiring a system safety group (SSG) meeting early in the program will help clarify system characteristics versus mission requirements and allow time to address issues. An additional SSG can be used to assure satisfactory closure of issues and smooth fielding of the system. Periodic SSGs through the remainder of the life cycle can be used to address on going concerns and special issues.

APPENDIX B

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

70. SUPPLEMENTARY REQUIREMENTS.

The contractor shall comply with the following requirements (as tailored **by the MA)** when this appendix is called out in the SOW.

70.1 Unacceptable/acceptable conditions.

70.1.1 Unacceptable conditions. The following safety critical conditions are considered **unacceptable.** Positive action **and implementation verification is required to reduce the risk to an acceptable level as** negotiated by the contractor and the **MA.**

a. Single component **failure,** common mode failure, human error, or design **features** which could cause a mishap of catastrophic or critical severity.

b. **Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of catastrophic or critical severity.**

c. Generation of hazardous ionizing/non-ionizing radiation or energy when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

d. Packaging or handling procedures and characteristics which could cause a mishap for which no controls have been provided to protect personnel or sensitive **equipment.**

e. Hazard level categories that are specified as unacceptable in the contract

70.1.2 **Acceptable conditions.** The following approaches are considered acceptable for correcting unacceptable conditions and will **require no** further analysis once controlling actions are **implemented and verified.**

a. For non safety critical command and control functions; a system design that requires two or more independent human errors, or that requires two or more independent failures, or a combination of independent failure and human error.

b. For safety critical command and control functions; a system design that requires at least three independent failures, or three human errors, or a combination of three independent failures and human errors.

c. System designs which positively prevent errors in assembly, installation, or connections which could result in a mishap.

d. System designs which positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause a mishap.

e. System design limitations on operation, interaction, or sequencing which preclude occurrence of a mishap.

f. System designs that provide an **approved safety factor, or fixed design allowance which limit, to an acceptable level, possibilities of structural failure or release of energy sufficient to cause a mishap.**

g. System designs that control energy build-up which could potentially cause a mishap (fuses, reliefvalves, electrical explosion proofing, etc.).

h. System designs in which component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin.

i. System designs which positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been provided.

j. System designs which limit/control the use ofhazardous materials.

70.2 Associate safety programs.

70.2.1 Industrial Safety and Hygiene. The contractor shall conduct the system safety program so that it supplements existing industrial safety and toxicology activities. This coordinated effort shall assure that government equipment or properties being used or developed under contract are protected from damage or mishap risk. When contractor owned or leased equipment is being used in manufacturing, testing or handling of products developed or produced under contract, analysis and operational proof checks shall be performed to show that risk of damage to those products has been minimized througb proper design maintenance, and operation by qualified personnel using approved procedures. This standard does not cover those functions the contractor is required by law to perform under Federal or State OSHA, DOT, or EPA regulations.

70.2.2 Operational site safety. The contractor system safety program shall encompass operational site activities. These activities shall include all operations listed in the operational time lines, including system installation, checkout, modification, and operation. Particular attention shall be given to operations and interfaces with ground support equipment and to the needs of the operators relating to personnel subsystems such as: panel layouts, individual operator tasks, fatigue prevention, biomedical considerations, etc.

70.2.3 Facilities. The contractor shall include facilities in the system safety analyses activity. Facility safety design criteria shall be incorporated in the facility specification. Consideration shall be given to the test, operational, and maintenance aspects of the program. Identified requirements will include consideration of the compatibility with standards equal to or *better* than those specified by the most stringent of Federal, State, Local and DOD Occupational Safety and Health Regulations. The test and operations safety procedures shall encompass all development, qualification, acceptance tests and operations. The procedures will include inputs from the safety analyses and will identify test, operations, facility, and support requirements. The procedures shall be upgraded and refined as required to correct deficiencies identified by the system safety analyses to incorporate additional safety requirements.

70.2.4 Range safety. Compliance with the design and operational criteria contained in the applicable range safety manuals, regulations, and standards shall be considered in the system safety analysis and the system safety criteria System safety is concerned with minimizing risk to on- or off-site personnel and property arising from system operations on a range.

70.2.5 Drone and Missile system safety.

APPENDIX C

a Verification of system design and operational planning compliance with range or operating site safety requirements shall be documented in the SAR or as otherwise specified in the contract SOW and CDRL.

b. Ensure that flight analysis and flight termination systems comply with the requirements of the test range being utilized. Such requirements are applicable to the system during all flight phases until vehicle/payload impact or orbital insertion. The SAR or other safety report as specified in the CDRL shall include all aspects of flight safety systems.

c. The contractor's system safety representative(s) will be an integral part of the flight evaluation and assessment team that reviews field/flight operations to correct any identified deficiencies and recommend appropriate safety enhancements during the field/flight operation process.

APPENDIX C

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D

80. DATA REQUIREMENTS FOR MIL-STD-882.

80.1 **Data Item Correlation.** Data item descriptions and the paragraphs of **MIL-STD-882** where their requirements are located are as follows:

Paragraph Location	DID No.
Task 101	**N/A**
Task 102	**DI-SAFT-80100A**
Task 103	**DI-SAFT-80100A**
Task 104	As per **CDRL**
Task 105	As per CDRL
Task 106	**DI-SAFT-80105A**
Task 107	**DI-SAFT-80105A**
Task 201	**DI-SAFT-80101A**
Task 202	**DI-SAFT-80101A**
Task 203	**DI-SAFT-80101A**
Task 204	**DI-SAFT-80101A**
Task 205	**DI-SAFT-80101A**
Task 206	**DI-SAFT-80101A**
Task 207	**DI-SAFT-80106A**
Task 301	**DI-SAFT-80102A**
Task 302	As per **CDRL**
Task 303	**DI-SAFT-80103A**
	DI-SAFT-80104A
Task 401	**DI-SAFT-80102A**
Task 402	**DI-SAFT-80102A**
Task 403	**DI-SAFT-81299**
Task 404	**DI-SAFT-80931**
Multiple Tasks	**DI-SAFT-81300**

NOTE: The latest version of each data item description required will be used unless an exception has been granted for a follow-on contract.

APPENDIX D

80.2 **Data Item Description (DID) List.**

a. DID's associated with this standard are the following:

1. DI-SAFT-80100A, "System Safety Program Plan."
2. DI-SAFT-80101A, "System Safety Hazard Analysis Report"
3. DI-SAFT-80102A, "safety Assessment Report"
4. DI-SAFT-80103A, "Engineering Change Proposal System Safety Report."
5. DI-SAFT-80104A, Waiver or Deviation System Safety Report."
6. DI-SAFT-80105A, "System Safety Program Progress Report."
7. DI-SAFT-80106A, "Health Hazard Assessment Report"
8. DI SAFT-80931, "Explosive Ordnance Disposal Data."
9. DI-SAFT-81299, "Explosive Hazard Classification Data"
10. DI-SAFT-81300, "Mishap Risk Assessment Report"

b. DID's which may be applicable to your system safety program but are not linked directly to this standard are as follows:

1. DI-ADMN-81250, "Conference Minutes." (May be used to acquire meeting minutes for Task 104 or 105.)
2. DI-H-1327A, "Surface Danger Area Data"
3. DI-H-1329A "Accident/Incident Report" (May be used to support Task 101 requirements for mishap/incident alerting notification, investigation, and reporting.)
4. DI-H-1332A, "Radioactive Material Data"
5. DI-HFAC-80938, "Noise Measurement Report"
6. DI-MISC-80043, "Ammunition Data Card." (For those contracts which will require shipment of explosive items to DoD facilities or locations.)
7. DI-MISC-80370, "Safety Engineering Analysis Report"
8. DI-R-7085A, "Failure Mode, Effects Criticality Analysis Report" (May be used to acquire the specific analysis technique report.)
9. DI-SAFT-80184, "Radiation Hazard Control Procedures"
10. DI-SAFT-81065, "Safety Studies Report"
11. DI-SAFT-81066, "Safety Studies Plan."

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given,
2. The submitter of this form must complete Mocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-STD 882C	2. DOCUMENT DATE (YYMMDD) 930119

3. DOCUMENT TITLE
SYSTEM SAFETY PROGRAM REQUIREMENTS

4. NATURE OF CHANGE (Identify paragraph number and include proposed rewrite, if possible Attach extra sheets as needed.)

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME (Last, First, Middle Initial)	b. ORGANIZATION	
c. ADDRESS (Include Zip Code)	d. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON (If applicable)	7. DATE SUBMITTED (YYMMDD)

8. PREPARING ACTIVITY

a. NAME	b. TELEPHONE (Include Area Code)	
CHUCK DORNEY	(1) Commercial (513) 257-6007	(2) AUTOVON 787-6007

ADDRESS (Include Zip Code)
HQ AFMC/SE
4170 Hebble Creek Rd Ste. 1
Wright Patterson AFB, OH 45433-5644

IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:
Defense Quality and Standardization Office
5203 Leesburg Pike, Suite 1403, fells Church. VA 22041.3466
Telephone (703) 756-2340 AUTOVON 289-2340